

# PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2000-187935

(43) Date of publication of application : 04.07.2000

(51) Int.Cl.

G11B 20/10  
G06F 12/14

(21) Application number : 11-202971

(71) Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22) Date of filing : 16.07.1999

(72) Inventor : TAGAWA KENJI  
MINAMI MASANAO  
KOZUKA MASAYUKI

(30) Priority

Priority number : 10206967 Priority date : 22.07.1998 Priority country : JP  
10289831 12.10.1998 JP

(54)

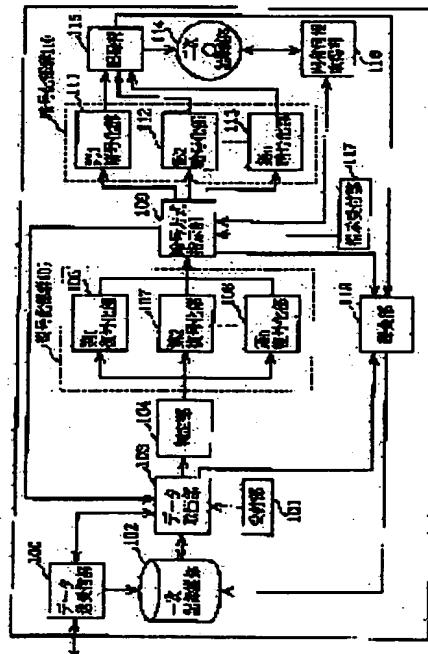
## DIGITAL DATA RECORDER, ITS METHOD AND COMPUTER READABLE RECORDING MEDIUM STORING ITS PROGRAM

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a digital data recorder protecting a copyright and facilitating the reproducing of the ciphered digital data.

**SOLUTION:** A data transmission and reception part 100 receives the electronically distributed ciphered digital data to record them in a primary recording medium. The cipher format of the digital data pulled out by a data pull-out part 103 is decided by a decision part 104 to be decoded by a proper decoding part. An intrinsic

information gain part 116 gains identification information of a secondary recording medium 114 or a reproducing device by whether or not the secondary recording medium is attachable or detachable for the reproducing device. A cypher system instruction part 109 selects one



cyphering part from plural cyphering parts according to the gained identification information. One cyphering part generates a cryptographic key based on the identification information to cipher the digital data. A recording part 115 records them in the secondary recording medium 114, and a charge part 118 charges according to charge information.

---

**LEGAL STATUS**

[Date of request for examination] 09.05.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than  
the examiner's decision of rejection or  
application converted registration]  
One

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

the  
eve  
app  
one  
[Da  
P  
Re

110  
8/2006  
app  
one  
[Da  
P  
Re

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-187935

(P2000-187935A)

(43)公開日 平成12年7月4日 (2000.7.4)

(51)Int.Cl.  
G 11 B 20/10  
G 06 F 12/14

識別記号  
320

F I  
C 11 B 20/10  
G 06 F 12/14

マークコード(参考)  
H  
320F

審査請求 未請求 請求項の数12 OL (全27頁)

(21)出願番号 特願平11-202971  
(22)出願日 平成11年7月16日 (1999.7.16)  
(31)優先権主張番号 特願平10-206967  
(32)優先日 平成10年7月22日 (1998.7.22)  
(33)優先権主張国 日本 (JP)  
(31)優先権主張番号 特願平10-289831  
(32)優先日 平成10年10月12日 (1998.10.12)  
(33)優先権主張国 日本 (JP)

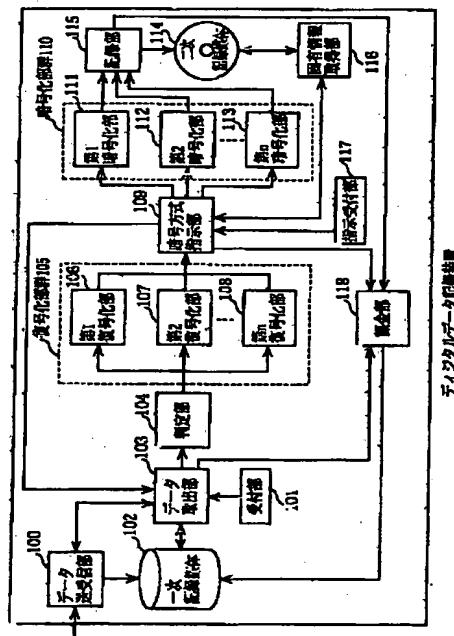
(71)出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(72)発明者 田川 健二  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72)発明者 南 賢尚  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72)発明者 小堀 雅之  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(74)代理人 100090446  
弁理士 中島 司朗 (外1名)

(54)【発明の名称】 デジタルデータ記録装置及びその方法並びにそのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】著作権を保護し、暗号化されたデジタルデータの再生を容易にするデジタルデータ記録装置を提供する。

【解決手段】データ送受信部100は、電子配信される暗号化されたデジタルデータを受信し、一次記録媒体に記録する。データ取出部103で取り出されたデジタルデータは、判定部104で暗号形式が判定され、適切な一の復号化部で復号される。固有情報取得部116は、二次記録媒体114が再生装置に対して着脱可能か否かで二次記録媒体114又は再生装置の識別情報を取得する。暗号方式指示部109は、取得された識別情報に従い、複数の暗号化部から一の暗号化部を選ぶ。一の暗号化部は、識別情報を基に暗号鍵を生成し、デジタルデータを暗号化する。それを記録部115は二次記録媒体114に記録し、課金部118は、課金情報に従い課金する。



## 【特許請求の範囲】

【請求項1】 ディジタルデータを記録媒体に記録するディジタルデータ記録装置において、暗号化されたディジタルデータをディジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化ディジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでディジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたディジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたディジタルデータを再暗号化させることを特徴とするディジタルデータ記録装置。

【請求項2】 前記記録媒体に記録されたディジタルデータは、再生装置により再生され、前記暗号化手段は、前記記録媒体の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第1暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第2暗号化部とを有し、前記制御手段は、前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第1暗号化部によりディジタルデータの暗号化を行わせ、着脱不可能なときは、前記第2暗号化部によりディジタルデータの暗号化を行わせることを特徴とする請求項1に記載のディジタルデータ記録装置。

【請求項3】 前記ディジタルデータ記録装置は、更に、前記ディジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求項1に記載のディジタルデータ記録装置。

【請求項4】 前記記録媒体に記録されたディジタルデータは、再生装置により再生され、前記暗号化手段は、

前記記録媒体の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第1暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第2暗号化部とを有し、前記制御手段は、

前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第1暗号化部によりディジタルデータの暗号化を行わせ、着脱不可能なときは、前記第

2暗号化部によりディジタルデータの暗号化を行わせることを特徴とする請求項3に記載のディジタルデータ記録装置。

【請求項5】 前記制御手段は、前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化ディジタルデータを、前記復号化手段により復号化することを禁止することを特徴とする請求項4に記載のディジタルデータ記録装置。

【請求項6】 前記暗号化手段の有する複数の暗号化部による暗号化されたディジタルデータは、前記通信手段により受信されたディジタルデータの暗号化に比べいずれもセキュリティレベルが低いことを特徴とする請求項1記載のディジタルデータ記録装置。

【請求項7】 前記通信手段により受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるディジタルデータは当該ディジタルデータの暗号化方式を示す属性情報を含み、

前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたディジタルデータをそれぞれ復号化し、前記制御手段は、前記通信手段により受信された暗号化ディジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化ディジタルデータを復号化するよう前記復号化手段を制御することを特徴とする請求項1に記載のディジタルデータ記録装置。

【請求項8】 前記ディジタルデータ記録装置は、更に、

前記ディジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、受信した暗号化ディジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求項7に記載のディジタルデータ記録装置。

【請求項9】 ディジタルデータを記録媒体に記録するディジタルデータ記録方法において、暗号化されたディジタルデータをディジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化ディジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたディジタルデータを暗号化する暗号化ステップと、

前記暗号化ステップにより暗号化されたディジタルデータを前記記録媒体に記録する記録ステップとを備えることを特徴とするディジタルデータ記録方法。

【請求項10】 前記通信ステップにより受信されるデ

イジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるディジタルデータは当該ディジタルデータの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたディジタルデータを復号化することを特徴とする請求項9に記載のディジタルデータ記録方法。

【請求項11】 ディジタルデータを第1記録媒体に記録するディジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、

暗号化されたディジタルデータをデジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化ディジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたディジタルデータを暗号化する暗号化ステップと、

前記暗号化ステップにより暗号化されたディジタルデータを前記第1記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項12】 前記通信ステップにより受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータは当該データの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたディジタルデータを復号化することをコンピュータに実行させるプログラムを記録した請求項11に記載のコンピュータ読み取り可能な記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】 本発明は、ディジタルデータの著作権保護を図るディジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体に関する。

##### 【0002】

【従来の技術】 近年のインターネットの普及により、PC(パーソナルコンピュータ)を用いて、ホームページ上から好みの音楽データなどをダウンロードにより入手し、クレジットカードなどの決済手段を通じて支払いを行う、いわゆるEC(ElectronicCommerce:電子商取引)による音楽流通が広がりつつある。このようなインターネットを通じたECによる音楽流通(以下「電子音楽配信」という。)が普及することは、ユーザーがレコード店に行く必要がなくなることを意味し、現在のCD(Compact Disc)を中心の音楽流通を大きく変えるものになる可能性を

持っている。

【0003】 ところで、音楽を鑑賞するスタイルという点に注目すると、自宅で鑑賞する以外にも、携帯型の再生装置を用いて、通勤、通学途中に鑑賞する、あるいは車の中で鑑賞するというスタイルもかなりの割合を占める。この場合には、音楽データをMD(Mini Disc)等の可搬型の媒体に記録する必要がある。また、電子音楽配信においては、各社それぞれ独自の暗号方式を採用し、著作権保護を図っている。すなわち、製作会社、流通経路、利用形態等に応じて、それぞれ異なる暗号方式を採用している。

##### 【0004】

【発明が解決しようとする課題】 このような状況において、電子音楽配信によって音楽データをMD等に記録する場合、流通段階での音楽データをそのまま記録したとき、MD等を再生する再生装置は、各暗号方式に対応して復号化できる装置が求められる。この結果、装置規模が大きくなり、価格の上昇を招き、ユーザにとっては不利益となる。

【0005】 一方、ユーザの利益だけを考えるなら、電子音楽配信された音楽データの暗号を復号化してMD等に記録するようにすれば、再生装置は、暗号解読を必要としないので安価なものを提供できることになる。しかしながら、この場合には、不正なコピーを助長して著作権保護を図ることができない。本発明は、上記課題に鑑みなされたものであり、著作権保護を図り、かつ記録媒体に記録された音楽データを安価なディジタルデータ再生装置で再生することができるディジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体を提供することを目的とする。

##### 【0006】

【課題を解決するための手段】 上記課題を解決するために、本発明は、ディジタルデータを記録媒体に記録するディジタルデータ記録装置において、暗号化されたディジタルデータをデジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化ディジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでディジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたディジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたディジタルデータを再暗号化させることとしている。

##### 【0007】

【発明の実施の形態】 以下、本発明に係るディジタルデータ記録装置の実施の形態について図面を用いて説明する。

(実施の形態1) 図1は、本発明に係るディジタルデータ

タ記録装置の実施の形態1の構成図である。このディジタルデータ記録装置は、データ送受信部100と、受付部101と、一次記録媒体102と、データ取出部103と、判定部104と、復号化部群105と、暗号方式指示部109と、暗号化部群110と、二次記録媒体114と、記録部115と、固有情報取得部116と、指示受付部117と、課金部118とを備えている。

【0008】なお、このディジタルデータ記録装置の二次記録媒体114と記録部115以外は、一般には図2に示すようにPC(パーソナルコンピュータ)201で実現され、記録部115は、例えばDVD(Digital Versatile Disc)-RAMドライブ202で、二次記録媒体114は、DVD-RAMディスク203でそれぞれ実現される。

【0009】このディジタルデータ記録装置は、インターネットを介して配信される暗号化されたディジタルデータである音楽データを受信し、一次記録媒体102にダウンロードした後、復号化部群105でディジタルデータを復号化し、暗号化部群110で再度暗号化したディジタルデータとして、記録部115で二次記録媒体114に記録する。

【0010】なお、本実施の形態では、電子音楽配信について説明するけれども、ディジタルデータの種類は、音楽データに限るものではなく、映像データ、文字データあるいはこれらの組み合わせでもよい。データ送受信部100は、モ뎀と制御ソフトで実現される通信部であり、電話回線を通じて情報提供者のホストコンピュータ(図示せず)に接続される。受付部101で受け付けられた希望する曲の購入要求をデータ取出部103にして通知されると、ホストコンピュータに送信する。インターネットを介して、ホストコンピュータから購入要求に従い配信される音楽データをダウンロードし、一次記録媒体102に記録する。また、曲を購入したときに生じる課金情報をホストコンピュータに送信する。

【0011】ここで、情報提供者が提供する情報について説明する。情報提供者は、曲販売のサイト、すなわち自社のホームページを開設しており、曲名、価格などユーザーの購入時に必要な情報、あるいは購買意欲をかきたてる情報を提供している。ユーザは、これらの情報提供者が提供する情報に基づいて、好みの曲を購入する。図3は、情報提供者が提供する情報、すなわち曲販売用のホームページの一例を示すものである。表示される情報としては、曲名301、歌手名302、収録時間303、価格304などの内容からなる。ここで、曲名301、歌手名302は、それぞれ、個々の音楽データの曲名、歌手名を表す情報である。収録時間303は、個々の曲の収録時間(再生時間)を示し、価格304は、個々の曲の販売価格を示している。これらの情報をもとに、ユーザは受付部101を通じて好みの曲を選択し、購入要求を通知することができる。もちろん、情報提供

者が提供する情報は、図3に示すように、文字情報に限られるものではなく、ジャケットピクチャのような画像や、試聴用の音楽データであってもよいことは言うまでもない。

【0012】受付部101は、キーボードやマウス等からなり、PCの表示画面に表示された図3に示した情報を見たユーザから音楽データの購入要求を受け付ける。受け付けた曲の購入要求は、データ取出部103を介して、データ送受信部100に通知される。一次記録媒体102は、一般にはPCのハードディスク等で実現され、データ送受信部100で受信された暗号化されたディジタルデータである音楽データを記憶している。また、一次記録媒体のセキュアな領域には、課金部118によって、ダウンロードされた音楽データを二次記録媒体114に記録したとき、例えば暗号化した課金データが記録される。

【0013】図4は、一次記録媒体102に記憶されているダウンロードした音楽データ、すなわち情報提供者が提供する音楽データのデータ構造の一例を示すものである。情報提供者が提供する音楽データは、大きく音楽データの曲名や歌手名、価格などの情報である属性情報401と、音楽データそのものである曲データ部402とから構成される。

【0014】属性情報401は、ISRC情報403、曲名404、歌手名405、価格406、情報提供者名407、暗号形式408から構成される。以下、これらの属性情報について説明する。ISRC(International Standard Recording Code)情報403は、音楽データごとに割り当たる固有の情報であって、国コード(2つのASCII文字)、オーナーコード(3つのASCII文字)、記録年(数字2桁)、シリアル番号(数字5桁)で構成される。曲名404、歌手名405は、それぞれ音楽データの曲名、歌手名を表す文字情報である。価格406は、音楽データの価格を表す情報である。なお、本実施の形態では、ダウンロードした音楽データをディジタルデータ記録装置を用いて、二次記録媒体に記録したときに請求される金額を示している。

【0015】情報提供者名407は、音楽データの提供者名、あるいは著作権者名を示す情報である。つまり、ユーザが本ディジタルデータ記録装置を用いて音楽データを記録したときに課金し、その金額をどの業者に振り分ければよいのかを示す情報である。暗号形式408は、ダウンロードした音楽データがどの暗号形式で暗号化されているかを示す情報である。すなわち音楽データは、情報提供者ごとに異なる暗号方式で暗号化されている。例えば、情報提供者A、情報提供者B、情報提供者Cが音楽データを提供する場合、情報提供者Aの提供する音楽データはA方式で暗号化されており、情報提供者Bの提供する音楽データはB方式で暗号化されており、情報提供者Cの提供する音楽データはC方式で暗号化さ

れている。なお、本実施の形態では、情報提供者の提供する情報が、さまざまな形式で暗号化されている場合に、それを記録した二次記録媒体114を再生装置で著作権の保護を図りつつ、容易に解読できる暗号形式に変換することが発明の主たる目的であり、暗号化のアルゴリズムの詳細な説明については省略する。

【0016】また、属性情報401においては、価格406、情報提供者名407は改竄されると情報提供者が不利益を被るおそれがあるため、必要に応じて暗号化されている。データ取出部103は、暗号方式指示部109からディジタルデータの取り出し指示を受けると、一次記録媒体102から、まず属性情報401を取り出し、属性情報401を課金部118に通知する。また、属性情報401中の暗号形式408の情報は、判定部104に通知する。なお、属性情報401中、価格406等が暗号化されているときは、復号化部群105によって、復号化してから課金部118に通知する。さらに一次記録媒体102から曲データ部402を取り出し、判定部104に出力する。データ取出部103で取り出されたデータは、すでに述べたように、情報提供者ごとに異なる暗号方式で暗号化されている。

【0017】判定部104は、データ取出部103から通知された暗号形式408の情報に基づいて、復号化部群105のいずれかの復号化部に音楽データを出力するか判定する。復号化部群105は、n個の復号化部よりなり、第1復号化部106はA方式で暗号化されたディジタルデータを復号し、第2復号化部107はB方式で暗号化されたディジタルデータを復号し、第n復号化部108はN方式で暗号化されたディジタルデータを復号する。各復号化部106～108は、情報提供者ごとの復号モジュールからなっている。

【0018】例えば、判定部104に通知された暗号形式408の情報がB方式であれば、判定部104は、音楽データの曲データ部402のディジタルデータを第2復号化部107に出力し、復号する。第2復号化部107は、入力されたディジタルデータを復号して、暗号方式指示部109に出力する。第1から第n復号化部106～108のいずれかにより暗号化されたデータを復号する際、復号鍵が必要であればデータ送受信部100でデータの暗号方式に応じた復号鍵入手し、データを復号化する。このようにして情報提供者ごとに異なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されているデータを復号化する。

【0019】暗号方式指示部109は、指示受付部117から暗号方式の種類の指示を受けているときは、その指示に従った固有情報の取得を固有情報取得部116に指示する。固有情報取得部116から指示した固有情報の通知を受けたときは、データ取出部103に音楽データの取り出しを指示する。固有情報取得部116から指示に従った固有情報を取得できない旨の通知を受けたと

きには、表示部(図示せず)に指示された暗号方式の種類では暗号化できない旨を表示させる。また、指示受付部117から暗号方式の種類の指示を受けていないときには、固有情報取得部116に二次記録媒体114の属性に従った固有情報の取得を指示する。固有情報取得部116から固有情報又は固有情報を取得できない旨を通知されると、データ取出部103に音楽データの取り出しを指示する。固有情報を取得できない旨の通知を受けたときには、乱数を発生する。

【0020】暗号方式指示部109は、指示受付部117から暗号方式の指示を受け付けているときは、その指示に応じた一の暗号化部を選び、復号化部群105のいずれかの復号化部106、107、…、108から復号されたディジタルデータの入力を受けると、固有情報取得部116から通知された固有情報とともに、復号されたディジタルデータを通知する。

【0021】また、暗号方式指示部109は、指示受付部117から指示を受け付けないときには、固有情報取得部116から通知された固有情報の種類に従い、一の暗号化部を選び、復号化部群105のいずれかの復号化部106～108から復号されたディジタルデータの入力を受けると、固有情報とともにディジタルデータを通知する。固有情報取得部116から固有情報を取得できない旨の通知を受けているとき、発生させた乱数とともに、一の暗号化部にディジタルデータを通知する。

【0022】暗号化部群110は、n個の暗号化部111、112、…、113からなる。各暗号化部111、112、…、113は、異なる種類の暗号鍵によって、通知されたディジタルデータを暗号化する。例えば、第1暗号化部111は、二次記録媒体114の固有の識別情報を基に作成される暗号鍵で暗号化する。第2暗号化部112は、二次記録媒体114を再生する再生装置(図示せず)の固有の識別情報を基に作成される暗号鍵で暗号化する。第n暗号化部113は、乱数を基に作成される暗号鍵で暗号化する。暗号化部111～113で用いられる各暗号鍵のデータサイズは、一次記録媒体102に記憶されている暗号化されたディジタルデータの暗号鍵のデータサイズよりも小さく設定される。

【0023】二次記録媒体114に記録される暗号化されたディジタルデータの暗号鍵のデータサイズが小さいことは、このディジタルデータを解読する際の困難性が低いことを意味する。したがって、二次記録媒体114を再生する再生装置でのディジタルデータの復号化に要する構成が簡単化されることになり、再生装置のコスト減につながる。

【0024】例えば、指示受付部117からの指示がないとき、暗号方式指示部109が固有情報取得部116から二次記録媒体の識別情報の通知を受けているときには、第1暗号化部111に二次記録媒体の識別情報を通知する。第1暗号化部111は、その識別情報を基に

暗号鍵を作成し、暗号方式指示部109から通知された音楽データの属性情報401の暗号形式408を書き換えるとともに、曲データ部402を、生成した暗号鍵で暗号化する。暗号化したディジタルデータを記録部115に通知する。

【0025】また、暗号方式指示部109は、指示受付部117から二次記録媒体114を再生する再生装置(図示せず)の固有情報による暗号化の指示を受けると、固有情報取得部116に再生装置の固有の識別情報を取得するよう指示する。固有情報取得部116から再生装置の固有の識別情報を通知されると、その識別情報と復号化部群105から通知された復号されたディジタルデータとを第2暗号化部112に通知する。

【0026】第2暗号化部112は、暗号方式指示部109から通知された識別情報を基に暗号鍵を生成し、生成した暗号鍵でディジタルデータを暗号化して記録部115に通知する。この際、音楽データの属性情報401の暗号形式408の内容を書き換えるのは、指示受付部117から指示を受け付けないときと同様である。二次記録媒体114は、例えば図2に示したDVD-RAMディスク、MD、再生装置(図示せず)の機種により埋め込み型あるいは取り外し可能な型の小型の半導体メモリ等からなり、暗号化部群110で暗号化された音楽データが記録部115によって記録される。例えば、DVD-RAMディスク203にディジタルデータが記録されていれば、図2に示すように、DVD-Audioプレーヤ204にDVD-RAMディスク203を挿入して音楽を聴取することができる。

【0027】記録部115は、例えば、図2に示したDVD-RAMドライブ202で実現され、暗号化部群110から通知されたディジタルデータを二次記録媒体114に記録する。また、記録が終了すると、その旨、課金部118に通知する。固有情報取得部116は、暗号方式指示部109から二次記録媒体114の固有の識別情報の取得を指示されたときには、例えば、DVD-RAMの場合はBCA(Burst Cutting Area)に書かれている情報を読み出し、通知する。なお、この二次記録媒体114の固有の識別情報は、媒体ごとにユニークであり、通常ディスクの製造時に記録される情報であって、ユーザーの通常の操作では読み出されたり、書き換えることができない。

【0028】したがって、この識別情報を基に暗号鍵を生成して、この暗号鍵で暗号化されたディジタルデータがDVD-RAMディスクに記録されるので、万一悪意を持ったユーザーがビットコピー可能なツールを用いてDVD-RAMディスクの内容を複製し、再生しようとしても、復号鍵の基になる情報が異なるため、正常に復号化することができない。この結果、音楽データの著作権を確実に保護することができる。

【0029】また、暗号方式指示部109から二次記録媒体114が装着された再生装置(図示せず)の固有の

識別情報の取得を指示されたときには、固有情報取得部116は、再生装置の識別情報を読み出し、暗号方式指示部109に通知する。この再生装置の固有の識別情報も再生装置の製造時に付される装置ごとのユニークな識別情報であるので、ユーザーの通常の操作では読み出されたり、書き換えられたりすることはできない。したがって、この識別情報を基に暗号化された場合も、特定の再生装置でしか再生することができない。

【0030】なお、固有情報取得部116は、暗号方式指示部109から指示された固有の識別情報を取得できないとき、即ち、二次記録媒体114又は再生装置に識別情報が付されていない場合には、指示された種類の固有の識別情報を取得できない旨を暗号方式指示部109に通知する。固有情報取得部116は、暗号方式指示部109から固有情報の種類の指示を受けずに、固有情報の取得の指示を受けると、二次記録媒体114がDVD-RAMディスクなどの再生装置から取り外し可能なものであるか、それとも、小型の半導体メモリのような再生装置に埋め込まれた取り外し不可能ものであるかを判断し、取り外し可能なものであれば、その二次記録媒体114の固有の識別情報を読み出し、暗号方式指示部109に二次記録媒体114の識別情報を通知し、取り外し不可能なものであれば、再生装置の識別情報を読み出し、同様に再生装置の識別情報を通知する。識別情報を取得できないときは、その旨を暗号方式指示部109に通知する。

【0031】指示受付部117は、PCのキーボードやマウスで実現され、ユーザーから暗号方式の種類の指示を受け付け、暗号方式指示部109に通知する。先に述べた図3に示すホームページの情報では、販売価格は1通りしかなかったけれども、図5に示すようなホームページの内容であれば、価格(1)501、価格(2)502の2通りの販売価格が示されている。

【0032】価格(1)501は、二次記録媒体114の固有の識別情報を基にディジタルデータを暗号化して記録するときの価格を示しており、価格(2)502は、二次記録媒体114を再生する再生装置の固有の識別情報を基にディジタルデータを暗号化して記録するときの価格を示している。なお、これらの2種類の価格は、情報提供者側でそれぞれ個別に自由に設定可能である。

【0033】ユーザーは、指示受付部117から二次記録媒体114の利用形態に応じて、図5に示す曲情報あるいはその価格情報を参照して好みの暗号形態でディジタルデータを暗号化することを指示することができる。例えば、特定の再生装置でのみ再生するとき、即ち、他の再生装置で二次記録媒体114を再生しないときには、再生装置の固有の識別情報を基に暗号化することを指示する。図5に示すように再生装置の識別情報を基に暗号化するほうが、価格(2)502に示すように一般的に

安価である。これは、他の再生装置で再生することができないので、二次記録媒体114の固有の識別情報を基に暗号化するよりも自由度が低いからである。ユーザは、自由に再生装置を選んで再生したいときには、二次記録媒体114の識別情報を基に暗号化するよう指示すればよい。

【0034】なお、指示受付部117と上述の受付部101とは、一体として構成されているけれども、説明上、2つの構成要素として説明した。課金部118は、データ取出部103から音楽データの属性情報401の通知を受け、記憶している。記録部115から暗号化されたディジタルデータを二次記録媒体114に記録した旨の通知を受けると、属性情報中の価格406を参照して課金額を決定し、一次記録媒体102のセキュアな領域に属性情報401とともに課金情報として書き込む。

【0035】なお、価格406が図5に示したように価格(1)501、価格(2)502のように複数あるときは、暗号方式指示部109から通知された第1から第n暗号化部111～113のいずれが利用されたかに従い課金額を決定する。次に、本実施の形態の動作を図6、図7のフローチャートを用いて説明する。先ず、受付部101はユーザからのホームページ表示の要求を受け、データ送受信部100が音楽データを提供する情報提供者が開設するホームページにアクセスし、データ取出部103によって表示部(図示せず)にホームページ(図3、図5参照)を表示させる(S602)。

【0036】次に、データ取出部103は、受付部101からユーザの希望する音楽データの購入指示を待ち、指定された音楽データの配信を受けるようデータ送受信部100に指示する(S604)。データ送受信部100は、音楽データを受信すると、一次記録媒体102にダウンロードする(S606)。ユーザは、ホームページの表示をみて、暗号方式の種類を二次記録媒体114の利用形態に応じて、指示受付部117から入力する。

【0037】暗号方式指示部109は、指示受付部117から暗号方式の種類の指示を通知されたか否か判断し(S608)、通知されたときは、指示された暗号方式の種類に用いる固有情報の取得を固有情報取得部116に指示する(S610)。固有情報取得部116から指示された固有情報を取得できない旨の通知を受けたか否かを判断し(S612)、その旨の通知を受けたときは、指示された暗号方式の種類では暗号化できない旨を表示部(図示せず)に表示させ(S614)、処理を終了する。指示した種類の固有情報の通知を受けたときには、データ取出部103にディジタルデータの取り出しを指示する。

【0038】データ取出部103は、一次記録媒体102に記録されている音楽データを取り出す(S616)。S608において、暗号方式指示部109は、指示受付部117から指示を通知されないと判断したと

き、固有情報取得部116に固有情報の種類を指定しないで、固有情報の取得を指示する(S618)。

【0039】固有情報取得部116は、二次記録媒体114の属性(再生装置(図示せず)に装着された二次記録媒体114が取り外し可能か不可能か)を判断し、取り外し可能な二次記録媒体114のときは二次記録媒体114の識別情報を取得し、取り外し不可能な二次記録媒体114のときは再生装置の識別情報を取得する(S620)。

【0040】暗号方式指示部109は、固有情報取得部116から取得された固有(識別)情報又は、固有情報を取得できなかったときはその旨の通知を受けると(S622)、データ取出部103にディジタルデータの取り出しを指示し、S616に移る。次に、判定部104は、データ取出部103で取り出された音楽データの属性情報401中の暗号形式408を参照して、復号化部群105のいずれの復号化部106～108で復号するかを判定する(S702)。

【0041】判定部104で判定された一の復号化部は、判定部104を介して入力されたディジタルデータを復号化し、復号したディジタルデータを暗号方式指示部109に出力する(S704)。暗号方式指示部109は、既に固有情報取得部116から通知されている固有情報(取得できない旨の情報も含む)に従い、暗号化部群110の一の暗号化部を選び、固有情報(取得できない旨の情報に対しては発生した乱数)と復号化されたディジタルデータとを通知する(S706)。

【0042】暗号方式指示部109から通知を受けた一の暗号化部は、固有(識別)情報に基づいて暗号鍵を生成し(乱数の通知に対しては乱数に基づいて暗号鍵を生成し)、ディジタルデータを暗号化する。この際、属性情報401のうち暗号形式408の内容も書き換えられる(S708)。記録部115は、第1～第n暗号化部111～113のいずれかから通知されたディジタルデータを二次記録媒体114に記録し(S710)、記録が終了すると課金部118に通知する。

【0043】課金部118は、記録部115から通知を受けると、データ取出部103から通知されている価格406等に従い課金額を決定し、課金情報を一次記録媒体102に記録して(S712)処理を終了する。上記実施の形態では、復号化部群105は、情報提供者ごとの復号モジュール(復号化部)からなるものとしたけれども、復号化部群は、音楽データの品質、例えば24ビットのLPCM(Liner Pulse Code Modulation)、MP3(Moving Picture Experts Group 1 Audio Layer 3)等のディジタルデータ、に応じて各復号化部を設けてよい。高品質の24ビットのLPCMは、解読の困難性の高い暗号化されたディジタルデータとし、通常品質のMP3は解読の困難性の低い暗号化されたディジタルデータとしておき、第1復号化部は24ビットのLPCMの

ディジタルデータを復号し、第2復号化部はMP3のデータを復号するようにしてもよい。

【0044】上記実施の形態では、暗号化部群110は、固有情報の種類で各暗号化部を設けたけれども、上述した品質に対応して、第1復号化部で復号化されたデータは第1暗号化部で暗号化し、第2復号化部で復号化されたデータは第2暗号化部で暗号化し、第n復号化部で復号化されたデータは第n暗号化部で暗号化するようにしてもよい。この場合、第1暗号化部で暗号化に用いる暗号鍵のデータサイズは、第2暗号化部のそれよりも大きく、第2暗号化部のそれは第n暗号化部のそれよりも大きく設定する。そして、課金部は、データを複合化部と復号化されたデータを再暗号化された暗号化部によって課金額を決定する。このようにすることによって、高品質の音楽データの方がより著作権の保護を確実なものとすることができる。また、この際、価格についても情報提供者は高品質の音楽データに高価格を設定することができる。

【0045】なお、上記実施の形態のデータ記録装置は、図1にその構成図を示したけれども、各構成要素の機能をコンピュータに発揮させるプログラムをコンピュータ読み取り可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないデータ記録装置に摘要して著作権の保護機能を有する装置とすることができる。

【0046】また、本実施の形態では、データはユーザーが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらず音楽データ、あるいは、属性情報のみをいったんユーザーのPC内の一次記録媒体102に記録しておき、一次記録媒体102に記録されているデータに対して購入手続きを行う形態も考えられる。

【0047】また、本実施の形態では、属性情報401は曲データ402と別個に記述するとして説明を行ったが、いわゆるWater Mark(電子すかし)の形式で曲データ402のデータ中に埋め込むことも可能である。また、本実施の形態において、復号化部群105と暗号化部群110との間の暗号方式指示部109を介してのデータ入出力に関しては特に言及していないが、セキュリティ上、認証を行ってデータを送信するか、あるいは復号化部群105、暗号方式指示部109及び暗号化部群110を1つのチップで実現する、といった方法で復号化されたデータの漏洩を防ぐようにしてもよい。

【0048】また、課金情報を記録するときには、一次記録媒体102中のセキュアな領域に記録するとして説明を行ったが、課金情報に関しては、一次記録媒体102とは別のICカードなどの記録媒体を設け、これに記

録することが可能である。本実施の形態では、課金のタイミングについては、説明を省略したが、例えば、データを二次記録媒体114に記録するときに必ずホストコンピュータと接続していなければいけないとするか、課金額が一定の金額に達するとホストコンピュータに自動的に接続するか、あるいは、課金情報記録後、一定の日時が経過すると自動的にホストコンピュータに接続する、としてもよい。

【0049】更に、本実施の形態では、情報提供者が提供する情報を音声情報として説明したが、これに限るものではなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報との組み合わせたものなどでもよいことはもちろんである。

(実施の形態2) 図8は、本発明に係わるデータ記録装置の実施の形態2の構成図である。このデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部2101、一次記録媒体2102、データ取出部2103、暗号方式判定部2104、第1の復号化部2105、第2の復号化部2106、第3の復号化部2107、暗号化部2108、記録部2109、二次記録媒体2110、入力部2111、表示部2112、記録媒体固有情報取得部2113を備える。また、復号化部群2115は、第1の復号化部2105、第2の復号化部2106、第3の復号化部2107から構成されるが、復号化部は3つに限るものではなく、ここでは、複数の復号化部から構成されることを示している。

【0050】なお、本実施の形態では、以後、記録対象となるデータを音楽データであるとし、音楽データはインターネットを通じて配信されるものとする。また、情報提供者ごとに異なる暗号方式でデータを暗号化しているものとする。情報提供者は、曲名、価格、コピー制御情報など(以後、属性情報と称する)購入時に必要な情報、あるいは購買意欲をかきたてる情報を音楽データに重畠または音楽データから分離して提供するものとするが、本実施の形態では、属性情報を音楽データから分離して提供する形態について説明する。

【0051】データ送受信部2101は、モデムで実現される通信部であり、電話回線を通じて提供者のホストコンピュータ(図示せず)に接続される。まず、ユーザーは情報提供者が提供する属性情報を取得する。データ送受信部2101により取得した属性情報は、一次記録媒体2102に記録され、その一部または全部が表示部2112に表示される。図9は、表示部2112に表示される情報の一例を示すものである。表示される情報としては、曲名2201、曲名コード2202、歌手名2203、データ入手先2204などの内容からなる。ここで、曲名2201、歌手名2203は、それぞれ音楽データに対する曲名、歌手名を表す情報である。曲名コード2202は、音楽データを他の音楽データと識別する

ための識別子であり、例えばISRC (International Standard Recording Code) 情報が付される。これらの情報をもとに、ユーザは入力部2111を通じて好みの曲を選択し、購入要求を通知することができる。データ入手先2204は、本実施の形態では該当する曲が記録されているURL (Uniform Resource Locator) 情報とする。もちろん、曲名コード2202にISRC情報が付されていれば、曲名コード2202からデータ入手先を特定することも可能である。

【0052】入力部2111は、マウス、キーボード等から実現され、ユーザからの曲の購入の指示、すなわち記録指示を受け付け、データ送受信部2101に通知する。ユーザは表示部2112に表示された情報を元に、マウスでその曲名等をクリックして音楽データの記録を指示する。入力部2111から音楽データの記録指示があると、データ送受信部2101から電話回線を通じて提供者のホストコンピュータから記録要求のあった曲をダウンロードする。この際に、属性情報中のURL情報をもとに曲データの位置を特定する。ダウンロードされたデータはいったん一次記録媒体2102に記録される。

【0053】一次記録媒体2102は、一般にはパソコンのハードディスクであって、ユーザが購入を希望した音楽データを暗号化されたまま記録する。したがって以後の動作に関しては、必ずしも常に提供者のホストコンピュータと接続している必要はない。データ取出部2103は、一次記録媒体2102から記録対象となる音楽データを取り出す。このとき、ユーザは表示部2112に表示される図9に示した情報と同程度の情報をもとに、二次記録媒体2110へ記録する音楽データを入力部2111を通じて選択する。データ取出部2103で取り出されたデータは、各情報提供者ごとの暗号方式で暗号化されている。このため、適当な復号方式で復号することを暗号方式判定部2104により判定する。具体的には、デジタルデータのヘッダ部に暗号方式を識別できる情報を附加して送信する、属性情報に暗号方式を記述しておく、などの方法が考えられ、これらの値に応じて暗号方式を判定する。

【0054】第1の復号化部2105、第2の復号化部2106、第3の復号化部2107は、各情報提供者ごとの復号方式が存在していることを示すものであって、必ずしも3つに限られるわけではない。暗号方式判定部2104により適当な復号化部を選択し、復号化部により暗号化されたデータを復号する。このとき、例えば暗号方式判定部2104で取得したデータの暗号方式に応じた復号鍵を入手または生成し、復号化部はこの復号鍵をもとにデータを復号化する。したがって、異なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されているデータを復号化することになる。

【0055】次に、暗号化部2108にて復号化された

データの暗号化を行うが、ここでは、記録媒体固有の固有情報を暗号鍵情報として暗号化を行うこととする。なお、記録媒体固有情報をもとに暗号化を行う一の方法について、特開平5-257816公報に開示されているので、ここでは詳しい説明は省略する。記録媒体固有情報取得部2113は、暗号化部2108からの指示に従い、二次記録媒体2110から固有情報を取り出し、暗号化部2108へ伝達する。

【0056】暗号化部2108は、記録媒体固有情報取得部2113で取得した固有情報を暗号鍵として、暗号化する。ここで、二次記録媒体2110固有の情報について説明する。二次記録媒体2110は、媒体ごとの固有の識別情報を持っている。これは例えばDVD-RAM (Digital Versatile Disc Random Access Memory) の場合、BCA (Burst Cutting Area) に書かれた情報に相当する。この情報は、ディスクごとにユニークであり、しかも通常ディスク製作時に記録される情報であって、書き換えることができない。したがって、万一悪意を持ったユーザがビットコピー可能なツールを用いてディスクの内容を複製したとしても、復号鍵のもとになる情報が異なるために復号化することができず、データの著作権を確実に保護することが可能となる。

【0057】記録部2109は、暗号化されたデータを二次記録媒体2110に記録する。以上のように構成されたディジタルデータ記録装置について、以後図10のフローチャートを用いてその動作を説明する。まず、データ送受信部2101は、属性情報をダウンロードし(S2301)、ユーザからのディジタルデータの記録指示を待ち(S2302)、指示されたディジタルデータをダウンロードし、一次記録媒体2102に記録する(S2303)。次に、ダウンロードしたデータの暗号方式を判定し、適当な復号化部2105~2107へ復号化を指示する(S2304)。復号化部2105~2107により復号化する(S2305)。暗号化部2108は、復号化されたデータが入力されると、記録媒体固有情報取得部2113から二次記録媒体2110の固有情報を取得する(S2306)。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部2108はデータを暗号化する(S2307)。記録部2109は、暗号化されたデータを二次記録媒体2110に記録し(S2308)、処理を終了する。

【0058】以上で、本発明の実施の形態2のディジタルデータ記録装置に関する説明を終わる。次に、本発明の実施の形態3のディジタルデータ記録装置に関する説明を行う。

(実施の形態3) 図11は、本発明に係わるディジタルデータ記録装置の実施の形態3の構成図である。このディジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部2101、一次記録媒体2102、データ取出部2103、暗号方式判定部

2104、復号化部群2115、属性情報取得部2401、コピー制御情報検出判定部2402、コピー制御情報変換部2403、課金情報算出部2404、暗号化部2108、記録部2109、二次記録媒体2110、入力部2111、表示部2112、記録媒体固有情報取得部2113を備える。

【0059】なお、実施の形態3では、実施の形態2のディジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。まず、本実施の形態において、記録対象となるデータの属性情報が図12の通りであるとする。図12に示す属性情報は、図9に示す属性情報に加えて、コピー制御情報2501、課金情報2502等の情報がある。ここで、コピー制御情報2501は、コピーが許可されている世代数、あるいは回数の情報からなる。例えば世代数に関しては、「無制限にコピー可」、「1世代だけコピー可（孫コピー禁止）」、「コピー禁止」等の値を取る。一方、回数に関しては、コピー許可されている回数のことと、0以上の整数値を取りうる。例えば「孫コピー不可」は、二次記録媒体2110にディジタルデータを記録後、二次記録媒体2110中のデータをもとにコピーすることを許可しないことを意味する。「無制限に許可」は、特に制限しないことを意味する。「2回コピー可」など、コピーの回数の情報が含まれる場合は、二次記録媒体2110に記録できる回数を意味する。

【0060】属性情報取得部2401は、一次記録媒体2102から、再生すべきデータに対応する属性情報を取得する。ここでは、コピー制御情報と課金情報を取り出す。なお、属性情報は著作権保護情報や課金情報を含むので、一次記録媒体2102中のセキュアな領域に記録して、ユーザの通常の操作ではアクセスできないことが望ましい。

【0061】コピー制御情報検出判定部2402は、属性情報中のコピー制御情報を取り出し、以後のコピーが許可されているかどうか、許可されているとすればその世代数、あるいは回数の情報を取得する。コピー制御情報検出判定部2403は、コピーが許可されている場合、コピー制御情報を必要に応じて書き換える。例えば、孫コピーが禁止されているときは、コピー制御情報の値を以後のコピーを禁止するように変更し、コピー許可回数が制限されているときは、許可回数から「1」減じた値に変更する。

【0062】ここで重要なのは、コピー許可回数が設定されているとき、一般に、一次記録媒体2102に記録されたデータを何回二次記録媒体2110にコピーさせるかという数値であるため、コピー制御情報の書き換え対象となるのは、一次記録媒体2102中に記録されているデータである。したがって、一次記録媒体2102中に記録されている。コピー許可回数を「1」減じた値に変更する。

た値に変換し、二次記録媒体2110に記録すべきコピー許可回数は0として記録する。

【0063】課金情報算出部2404は、属性情報取得部2401で取得した属性情報から該当する曲の課金情報を取得し、これをもとに課金額を算出し、一次記録媒体2102中のセキュアな領域に記録する。以上のように構成されたディジタルデータ記録装置について、以下、図13および図14のフローチャートを用いてその動作を説明する。

【0064】まず、データ送受信部2101は、属性情報をダウンロードし(S2601)、ユーザからのディジタルデータの記録指示を持ち(S2602)、指示されたディジタルデータをダウンロードし、一次記録媒体2102に記録する(S2603)。次に、記録対象となるデータの属性情報を属性情報取得部2401により取得する(S2604)。コピー制御情報判定部2402により属性情報中のコピー制御情報を判定し、コピーが許可されているかどうかを判定する(S2605)。コピーが許可されているときは、コピーが許可されている世代、回数の情報を取得し、必要に応じてコピー制御情報変換部2403で書き換える(S2606)。コピーが許可されていない場合は、以後の処理を中断する(S2607)。次に暗号方式を判定し、復号化群2115中の適当な復号化部へ復号化を指示する(S2608)。復号化部2105～2107により復号化を行う(S2609)。復号化が終わると、属性情報取得部2401で取得した属性情報中の課金情報から適切な課金額を算出する(S2610)。

【0065】暗号化部2108は、復号化されたデータが入力されると、記録媒体固有情報取得部2113から二次記録媒体2110の固有情報を取得する(S2611)。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部2108はデータを暗号化する(S2612)。記録部2109は、暗号化されたデータを二次記録媒体2110に記録し(S2613)、処理を終了する。

【0066】以上で、本発明の実施の形態3に関する説明を終わる。

(実施の形態4) 次に、本発明に係わるディジタルデータ記録装置の実施の形態4について説明する。このディジタルデータ記録装置は、実施の形態2とほぼ同一であるが、固有情報取得送出部2803、記録部2109、二次記録媒体2110が第2のディジタルデータ記録装置内にある点と、暗号鍵の情報のみが異なる。図15は、本発明に係わるディジタルデータ記録装置の実施の形態4の構成図である。このディジタルデータ記録装置は、第1のディジタルデータ記録装置2800と、第2のディジタルデータ記録装置2801とからなる。

【0067】第1のディジタルデータ記録装置2800は、データ送受信部2101、一次記録媒体2102、

データ取出部2103、暗号方式判定部2104、復号化部群2115、暗号化部2108、入力部2111、表示部2112、固有情報取得部2802備える。第2のディジタルデータ記録装置2801は、固有情報取得送出部2803、記録部2109、二次記録媒体2110を備える。

【0068】なお、実施の形態4では、実施の形態2のディジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。暗号化部2108へ復号化部群2115にて復号されたデータが入力されると、記録媒体固有情報取得部2802は、第2のディジタルデータ記録装置2801中の固有情報取得送出部2803へ固有情報の送出要求を出す。固有情報取得送出部2803は、第2のディジタルデータ記録装置2801に装着されている二次記録媒体2110の固有識別情報、あるいは第2のディジタルデータ記録装置2801固有の識別情報の組み合わせの情報を暗号鍵の一部としてデータを暗号化し、第2のディジタルデータ記録装置2801へ出力する。第2のディジタルデータ記録装置2801中の記録部2109は暗号化されたデータを二次記録媒体2110へ記録する。

【0070】なお、固有情報取得送出部2803で取得送出する固有情報であるが、二次記録媒体2110が第2のディジタルデータ記録装置2801に固定的に設けられているときは、装置固有の識別情報とし、二次記録媒体2110が着脱自在に設けられているときは、二次記録媒体2110固有の固有情報、あるいは二次記録媒体2110の固有識別情報と第2のディジタルデータ記録装置2801固有の識別情報の組み合わせの情報をすることにより、より柔軟な暗号方式を使用することが可能になる。

【0071】以上で、実施の形態4の説明を終わる。  
 (実施の形態5) 次に、本発明に係わるディジタルデータ記録装置の実施の形態5について説明する。このディジタルデータ記録装置は、実施の形態2、3および4とほぼ同一である。ここでは、実施の形態4の説明に用いた構成図、図15を用いて説明する。相違点は、二次記録媒体2110に応じた暗号形式を採用し、記録することである。つまり、DVD-RAMと半導体メモリとでは取り扱うデータの最小単位、暗号化データを書きこむデータ量の単位の単位が異なるため、固有情報取得部2802は、固有情報取得送出部2803から、媒体の情報も取

得して、最適なデータの単位で暗号化を行なうことになる。このため、暗号化部2108が複数存在し、適切な暗号化部へ固有情報ならびに媒体情報も伝達するものである。以上より、DVD-RAMに限らず、半導体メモリ、ICカード、ハードディスク等を二次記録媒体2110として使用することが可能となる。

【0072】以上で、実施の形態5の説明を終わる。なお、上記実施の形態2～5は現状において最善の効果が期待できるシステム例として説明したにすぎない。本発明は、その要旨を逸脱しない範囲で実施変更することができる。具体的には以下に示すような変更実施が可能である。また、実施の形態2～5では、ディジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらずいったんユーザのPC内の一次記録媒体2102に記録しておき、一次記録媒体2102に記録されているディジタルデータに対して購入手続きを行う形態も考えられる。

【0073】また、実施の形態2～5では、コピー制御情報を属性情報に記述するとして説明を行なったが、いわゆるWaterMark(電子すかし)の形式でディジタルデータ中に埋め込むことも可能である。また、課金情報を記録するときには、一次記録媒体2102中のセキュアな領域に記録するとして説明を行なったが、課金情報に関しては、一次記録媒体2102とは別のICカードなどの記録媒体を設け、これに記録することが可能である。

【0074】また、実施の形態2～5では、情報提供者が提供する情報を音声情報として説明したが、これに限るものではなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報の組み合わせたものなどでもよいことはもちろんである。

(実施の形態6) 図16は、本発明に係るディジタルデータ記録装置の実施の形態6の構成図である。

【0075】このディジタルデータ記録装置は、通信部3101と、記録媒体3102と、受信データ記録判定部3103と、表示部3104と、入力操作部3105と、記録媒体固有情報取得部3106と、暗号化部3107と、記録部3108と、課金情報記録部3109と、課金情報記録媒体3110と、課金部3111とを備えており、PCで実現される。

【0076】通信部3101は、モデムで実現され、電話回線を介してデータ提供者のホストコンピュータ(図示せず)及び課金センタ(図示せず)に接続される。ホストコンピュータからディジタルデータとその属性情報とを受信すると、受信データ記録判定部3103に通知する。また、通信部3101は、課金センタから利用料の問い合わせがあると、その旨課金部3111に通知し、課金部3111から課金情報の通知を受けると、電話回線を介して、課金センタに課金情報を通知する。

【0077】本実施の形態では、データ提供者が提供するディジタルデータを音楽データであるとして説明する。データ提供者は、提供する音楽データを必要に応じて暗号化したディジタルデータとし、ディジタルデータには、情報識別子が付されている。情報識別子は、曲名コードであり、他の音楽と識別するためのものである。また、ディジタルデータには、属性情報が付加されている。属性情報は、ディジタルデータの利用料金等を示すものであり、どの情報提供者から提供された情報であるかを示す情報も含まれている。

【0078】図1-7は、属性情報の内容の一例を示す図である。属性情報3201には、ディジタルデータの曲名3202、演奏者（歌手）3203、曲名コード3204、記録料金3205、1回あたりの再生料金3206、再生可能回数3207、暗号状態3208、コピー許可3209等の項目の内容が含まれる。ここで、曲名3202、演奏者3203は、表示部3104に表示して、ユーザがコピー（複製）をするか否かを指示する判断資料となるものである。曲名コード3204は、音楽データを他の音楽データと識別するための識別子であり、曲ごとにユニークなものであり、例えばISRC（International Standard Recording Code）が付される。なお、このコードは国コード（2つのASCII文字）、オーナーコード（3つのASCII文字）、記録年（数字2桁）、シリアル番号（数字5桁）で構成されている。

【0079】記録料金3205、1回あたり再生料金3206、再生可能回数3207等は、課金基準データを構成し、いずれもその音楽データの利用料金を算定する為の情報である。記録料金3205は、通信部3101で受信されたディジタルデータを記録媒体3102に記録する際の料金である。1回あたりの再生料金3206は、記録媒体3102に記録されたディジタルデータの再生1回あたりの料金を示している。再生可能回数3207は、記録媒体3102に記録されたディジタルデータの再生が許容される回数を示している。「100回」と記録されているときには、100回に限り再生できることを示している。また、再生回数が一定回数以上になると、その後の料金が不要となる買い取り形式の設定也可能である。

【0080】暗号状態3208は、暗号有無フラグであり、通信部3101で受信されたディジタルデータが暗号化されているか否かを示すものである。コピー許可3209は、記録許可フラグであり、ユーザ側で記録する、即ち、記録媒体3102に受信された音楽データを記録することを許可するか否かを示す情報である。「1回のみ可」とは、1度だけ記録することが許可され、「許可」は、何度も記録することが許可されていることを示している。

【0081】なお、本発明は、受信された音楽データを

記録媒体3102に記録（複製）し、再生するときの音楽の著作権保護を図ることを主目的としたものであるので、この音楽データをリアルタイムに聴取するだけが許可されている場合についての説明は、簡単にする。この場合は、コピー許可3209は、「不可」とされている。このディジタルデータ記録装置には、復号化部と出力部とがその構成から省略されているけれども、通信部3101で受信されたディジタルデータは復号化部で復号され、出力部から音楽が出力される。この際、課金基準データには、聴取料金が含まれている。

【0082】記録媒体3102は、書き換え可能な記憶部材からなり、装置本体に着脱可能に取り着けられており、例えば、DVD-RAM等で構成される。記録媒体3102の書き換え不能なセキュアな領域には、記録媒体3102の固有情報が予め記録されている。また、記録媒体3102には、記録部3108によって、暗号化部3107で暗号化されたディジタルデータが記録される。

【0083】更に、記録媒体3102には、記録されたディジタルデータの管理情報と属性情報とが記録部3108によって記録されている。受信データ記録判定部3103は、通信部3101からディジタルデータとその属性情報3201との通知を受けると、その属性情報3201を最初に通知されたとき記憶し、属性情報のうち、曲名3202、演奏者3203、記録料金3205、1回あたり再生料金3206等を表示部3104に表示させ、ディジタルデータを暗号化部3107に通知する。

【0084】入力操作部3105からコピー（複製）指示を受けると、指示された音楽の曲名コード3204のディジタルデータのコピーが可能か否かを属性情報3201のコピー許可3209を見て判断する。コピーが許可であれば、記録媒体固有情報取得部3106に記録媒体3102の固有情報を取得するよう指示する。また、暗号化部3107に曲名コード3204と暗号状態3208を通知する。

【0085】コピーが不可であれば、表示部3104にその旨を表示させる。受信データ記録判定部3103は、記録部3108からコピー終了の通知を受けると、記憶している属性情報3201の項目、コピー許可3209を書き換える。即ち、コピー許可3209が「1回のみ」とされているときには「コピー不可」に、「何回のみ可」と数字が記録されているときには「1」を減じた数字にそれぞれ書き換える。なお、この属性情報3201を記憶する記憶領域は、EEPROM内に設けられており、このディジタルデータ記録装置の電源がオフされた場合でも記憶内容は消失しない。

【0086】例えば、暗号化部3107に曲名コード3204の「song01」を通知した後に、記録部3108からコピー終了の通知を受けると、「song01」に対応する項目、コピー許可3209を「1回のみ可」から「コピ

一不可」に書き換える。このようにすることによってデータ提供者の有する権利が侵されることを防止できる。

【0087】表示部3104は、液晶ディスプレイやCRT等からなり、受信データ記録判定部3103の制御により、デジタルデータである音楽データの曲名等の表示や、コピーができない旨の表示をする。入力操作部3105は、マウス等からなり、ユーザのコピー指示を受け付け、受信データ記録判定部3103に通知する。ユーザは、表示部3104に表示された曲名や演奏者の表示を見て、記録媒体3102にその音楽をダウンロードしようとするとき、マウスでその曲名等をクリックして、その音楽のコピーを指示する。

【0088】記録媒体固有情報取得部3106は、受信データ記録判定部3103から固有情報の取得指示を受けると、記録媒体3102のセキュアな領域に記録されている固有情報を読み出し、暗号化部3107に通知する。暗号化部3107は、記録媒体固有情報取得部3106から通知された固有情報を基に暗号鍵を作成する。受信データ記録判定部3103から通知されたデジタルデータを作成した暗号鍵を用いて暗号化したデジタルデータを作成し、記録部3108に通知する。

【0089】なお、受信データ記録判定部3103から通知されたデジタルデータが暗号化されている旨の通知を受けている場合には、そのデジタルデータを復号化しておいてもよいし、そのままの状態でもよい。例えば、記録媒体3102に記録すべきデジタルデータdataAを受信データ記録判定部3103から通知された場合に、記録媒体3102の固有情報を基に暗号鍵KMを作成すると、暗号化したデジタルデータE(KM.dat.aA)を作成する。他の記録媒体にデジタルデータdat.aAを記録する場合には、その他の記録媒体の固有情報を基に暗号鍵'KMを作成したときは、暗号化したデジタルデータEは、E(K'M,dataA)となる。

【0090】ここで、デジタルデータの暗号化の技術については、特開平5-257816号公報に記載されている。記録部3108は、暗号化部3107から通知された暗号化されたデジタルデータを記録媒体3102に記録する。この際、記録媒体3102に記録したデジタルデータの管理情報を作成して、記録媒体3102に記録する。

【0091】図18は、管理情報の一例を示す図である。管理情報3301には、記録したデジタルデータの識別子である曲名コード3204と、記録媒体3102に記録されたデジタルデータの記録開始アドレス3302、記録終了アドレス3303とが対応して記録される。記録媒体3102に記録されたデジタルデータを再生する際、この管理情報3301が参照される。

【0092】また、記録部3108は、記録媒体3102に暗号化されたデジタルデータ及び管理情報の記録が終了すると、受信データ記録判定部3103に記憶さ

れている記録したデジタルデータに対応する属性情報3201を読み出し、記録媒体3102に書き込む。更に、受信データ記録判定部3103にコピー終了の通知をする。また、課金情報記録部3109に、記録したデジタルデータの曲名コードを通知する。

【0093】課金情報記録部3109は、記録部3108から曲名コード3204の通知を受けると、受信データ記録判定部3103に記憶されている曲名コード3204に対応する属性情報3201の記録料金3205を読み出し、記録料金が有料のときは、課金情報記録媒体3110にその曲名コードと記録料金と記録日時等を課金情報として記録する。

【0094】課金情報記録媒体3110は、RAMカード等からなり、記録媒体3102にダウンロードしたデジタルデータの課金情報が課金情報記録部3109によって記録される。課金部3111は、通信部3101を介して課金センタ(図示せず)からの利用料の問い合わせがあると、課金情報記録媒体3110に記録されている未決済の課金情報を読み出し、通信部3101に通知する。通知が終了すると、課金センタに通知済(決済)のフラグを課金情報記録媒体3110に記録する。

【0095】次に、本実施の形態の動作を図19のフローチャートを用いて説明する。先ず、受信データ記録判定部3103は、ユーザからデジタルデータの記録指示を待ち(S3402)、指示されたデジタルデータのコピーが許可されているか否かを属性情報201を見て判断する(S3404)。否のときは、コピーが許可されていない旨を表示部3104に表示させ(S3406)、処理を終了する。

【0096】コピーが許可されているときは、記録媒体固有情報取得部3106は、記録媒体3102のセキュアな領域に記録されている記録媒体3102の固有情報を取得し、暗号化部3107に通知する(S3408)。暗号化部3107は、固有情報を基に暗号鍵を作成し、デジタルデータを暗号化する(S3410)。

【0097】記録部3108は、暗号化されたデジタルデータを記録媒体3102に記録する(S3412)。次に、課金情報記録部3109は、記録されたデジタルデータの記録料金が有料か否かを判断する(S3414)。無料であれば、処理を終了し、有料であれば、課金情報記録媒体3110に課金情報を記録して(S3416)、処理を終了する。

【0098】図20は、上述のデジタルデータ記録装置で記録媒体3102に記録されたデジタルデータの再生装置の構成図である。このデジタルデータ再生装置は、記録媒体3102と、入力操作部3501と、再生情報読出部3502と、表示部3503と、記録媒体固有情報取得部3504と、復号化部3505と、再生部3506と、課金情報記録部3507と、課金情報記録媒体3508とを備えている。

【0099】記録媒体3102は、上記ディジタルデータ記録装置で暗号化されたディジタルデータと管理情報3301と属性情報3201とか記録されたDVD-RAMを識別する識別子である固有情報が記録されている。入力操作部3501は、ユーザから再生開始の指示を受けると、再生情報読出部3502に初期起動の指示を与える。ユーザから曲名の指示を受けると、その曲名を再生情報読出部3502に通知する。なお、初期起動の指示の他に記録媒体3102がこのディジタルデータ再生装置に挿入されたときにも自動再生モードの指示が再生情報読出部3502に与えられる。

【0100】再生情報読出部3502は、入力操作部3501から初期起動の指示を受けると、記録媒体3102に記録されている属性情報3201を読み出し、その項目である曲名3202及び演奏者3203の一覧を表示部3503に表示させる。また、入力操作部3501から曲名の指示又は、自動再生モードの指示を受けると、属性情報3201の対応する再生可能回数3207が「1」以上であるか否かを判断する。再生可能回数3207が「1」以上であれば、その曲名コード3204を読み出し、管理情報3301の記録開始アドレスから記録終了アドレスまでに記録された暗号化されたディジタルデータを読み出し、復号化部3505に通知する。この際、記録媒体固有情報取得部3504に固有情報を取得するよう指示するとともに、課金情報記録部3507に、曲名コード3204と1回あたりの再生料金3206とを通知する。更にディジタルデータの読み出しが終了すると、属性情報3201の項目である再生可能回数3207の数を「1」減じた数に書き換える。なお、再生可能回数3207が「無限」の場合には、そのままにする。

【0101】再生情報読出部3502は、再生可能回数が「1」未満であると判断したとき、表示部3503に再生可能回数が越えた旨を表示させる。表示部3503は、液晶ディスプレイ等からなり、再生情報読出部3502で読み出された曲名等を一覧表示する。また、再生可能回数を超えてのユーザからの曲名指定に対して、再生可能回数が越えた旨を表示する。

【0102】記録媒体固有情報取得部3504は、再生情報読出部3502から固有情報の取得を指示されると、記録媒体3102のセキュアな領域から記録媒体3102の識別子である固有情報を取得し、復号化部3505に通知する。復号化部3505は、記録媒体固有情報取得部3504から固有情報の通知と、再生情報読出部3502から暗号化されたディジタルデータの通知とを受けると、固有情報を基に復号鍵を作成して、暗号化されたディジタルデータを復号し、復号化したディジタルデータを再生部3506に通知する。

【0103】再生部3506は、復号化部3505からディジタルデータの通知を受けると、デコードして音楽

を再生する。音楽の再生を終了すると課金情報記録部3507に再生終了を通知する。課金情報記録部3507は、再生部3506から再生終了の通知を受けると、再生情報読出部3502から通知されている曲名コード3204と1回あたりの再生料金3206と再生日時とを課金情報として課金情報記録媒体3508に記録する。なお、1回あたりの再生料金3206が有料でなければ、記録はしない。

【0104】課金情報記録媒体3508は、RAMカード等からなり、課金情報を課金情報記録部3507によって記録される。次に、このディジタルデータ再生装置の動作を図21に示すフローチャートを用いて説明する。先ず、ユーザは、再生開始を入力操作部3501のリモコン等を用いて指示し、表示部3503に表示された曲名を指定する。再生情報読出部3502は、音樂の再生要求であるとし(S3602)、指定された曲名の再生可能回数が「1」以上であるか否かを属性情報3201をみて判断する(S3604)。再生可能回数が「1」未満であれば、表示部3503に再生可能回数を超えた旨を表示させ(S3606)、処理を終了する。

【0105】再生可能回数が「1」以上の場合には、再生情報読出部3502は、記録媒体3102から暗号化されたディジタルデータを読み出し、復号化部3505に通知する(S3608)。記録媒体固有情報取得部3504は、記録媒体3102から固有情報を取得して復号化部3505に通知する(S3610)。

【0106】復号化部3505は、固有情報を復号鍵として暗号化されたディジタルデータを復号化する(S3612)。再生部3506は、ディジタルデータをデコードして音楽を再生出力する(S3614)。課金情報記録部3507は、再生料金が有料であるか否かを判断し(S3616)、無料のときは何もせずに、有料のときは、課金情報を課金情報記録媒体3508に記録して(S3618)、処理を終了する。

【0107】(実施の形態7)図22は、本発明に係るディジタルデータ記録装置の実施の形態7の構成図である。このディジタルデータ記録装置は、第1ディジタルデータ記録装置3700と第2ディジタルデータ記録再生装置3710とからなる。第1ディジタルデータ記録装置3700は、第1記録媒体3701と、通信部3101と、受信データ1次記録判定部3702と、表示部3104と、入力操作部3105と、1次記録部3703と、受信データ読出判定部3704と、固有情報取得部3705と、暗号化部3706と、課金情報記録部3109と、課金情報記録媒体3110と、課金部3111とを備えており、PCで実現される。

【0108】第2ディジタルデータ記録再生装置3710は、固有情報取得送出部3707と、2次記録部3708と、第2記録媒体3709と、入力操作部3501と、再生情報読出部3502と、表示部3503と、復

号化部3505と、再生部3506と、課金情報記録部3507と、課金情報記録媒体3508とを備えている。

【0110】なお、上記実施の形態6のディジタルデータ記録装置及びディジタルデータ再生装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分についてのみ説明する。先ず、第1ディジタルデータ記録装置3700について説明する。上記実施の形態6のディジタルデータ記録装置と異なるのは、第1記録媒体3701が本装置に固定的に設けられ、この第1記録媒体3701に記録されたディジタルデータが2次記録のために暗号化されて出力されることである。

【0110】第1記録媒体3701は、本装置3700内に固定的に設けられたハードディスク等の書き込み可能な記録部材からなる。第1記録媒体3701には、通信部3101で受信された音楽データであるディジタルデータとその管理情報とが1次記録部3703によって書き込まれる。受信データ1次記録判定部3702は、通信部3101で受信されたディジタルデータに付された属性データをEEPROM内に設けられた記憶領域に書き込む。本実施の形態で受信される属性情報の一例を図23に示す。属性情報3801は、上記実施の形態6の属性情報3201と2次記録料金3802が記録されていることと、コピー許可(1次)3803と(2次)3804との記録の許可回数が示されていることが異なる。

【0111】また、曲名コード「song05」の「曲E」では、コピーが1次、2次ともに不許可であり、リアルタイムの聴取のみが許可された音楽であることを示している。受信データ1次記録判定部3702は、ユーザからある音楽の2次記録の指示を受けると、先ず1次記録が許可されているか否かを属性情報3801の項目コピー許可(1次)3803を見て判断する。許可されていないときは、表示部3104に不許可である旨を表示させる。許可されているときは、指示された音楽のディジタルデータを1次記録部3703に通知する。他の機能は、上記実施の形態6の受信データ記録判定部3103と同様である。

【0112】1次記録部3703は、通知されたディジタルデータを第1記録媒体3701に記録する。この際、管理情報を書き込むのは、上記実施の形態6の記録部3108と同様である。なお、上記実施の形態6では、記録媒体3102の固有情報を基に暗号鍵が作成され、ディジタルデータが暗号化されていたけれども、本実施の形態では、第1記録媒体3701が除外され、他の装置で利用されることがないので暗号化されない。

【0113】また、1次記録部3703は、第1記録媒体3701へのディジタルデータの記録が終了すると、受信データ読出判定部3704に記録した曲名コード3

805を通知する。受信データ読出判定部3704は、1次記録部3703から曲名コード3805の通知を受けると、その音楽の2次記録が許可されているか否かを、受信データ1次記録判定部3702の属性情報3801中のコピー許可(2次)3804を見て判断する。許可されていないとき、又は、許可回数が「1」以上でないときには、表示部3104に2次記録が許可されていない旨を表示させる。

【0114】受信データ読出判定部3704は、2次記録が許可されているときには、管理情報(図18参照)を見て、第1記録媒体3701に記録されている通知された曲名コードのディジタルデータを読み出して暗号化部3706に通知するとともに、固有情報取得部3705に固有情報を取得するよう指示する。また、受信データ読出判定部3704は、ディジタルデータの読み出しが完了すると、受信データ1次記録判定部3702に記憶されている属性情報3801のコピー許可(2次)3804の回数から「1」減じた数に書き換える。例えば「1回のみ可」であれば「不許可」に書き換え、「許可」だけであれば、回数に制限がないので、そのまま書き換えは行わない。

【0115】なお、受信データ読出判定部3704は、暗号化部3706にディジタルデータの通知の後に、受信データ1次記録判定部3702に記憶されている属性情報を読み出して通知する。固有情報取得部3705は、受信データ読出判定部3704から固有情報を取得するよう指示されると、第1ディジタルデータ記録装置3700に接続されている第2ディジタルデータ記録再生装置3710の固有情報取得送出部3707に、固有情報の送出を要求する。固有情報取得送出部3707から固有情報の通知を受けると、暗号化部3706に固有情報を通知する。

【0116】暗号化部3706は、固有情報取得部3705から通知された固有情報を基に暗号鍵を作成し、受信データ読出判定部3704から通知されたディジタルデータを暗号化して第2ディジタルデータ記録再生装置3710の2次記録部3708に送出する。この暗号化されたディジタルデータの送出の後に、通知された属性情報も送出する。

【0117】次に、第2ディジタルデータ記録再生装置3710について説明する。この第2ディジタルデータ記録再生装置3710は、携帯型の例えばヘッドフォンステレオタイプの装置で実現される。また、第2記録媒体3709がこの装置3710から着脱自在の半導体メモリのICカード等から構成されている。固有情報取得送出部3707は、第1ディジタルデータ記録装置3700の固有情報取得部3705から固有情報の送出要求を受けると、第2記録媒体3709に予め記録されている第2記録媒体固有の媒体識別情報と、この装置3710固有の機器識別情報を取得して、固有情報取得部3

705に通知する。また、再生情報読出部3502から固有情報の通知指示を受けると、復号化部3505に媒体識別情報と機器識別情報とを通知する。

【0118】2次記録部3708は、第1ディジタルデータ記録装置3700の暗号化部3706から暗号化されたディジタルデータと、属性情報との出力を受けると、第2記録媒体3709に記録する。併せて、図18に示したような管理情報3301を記録する。復号化部3505は、固有情報取得送出部3707から通知された媒体識別情報と機器識別情報との2つの情報を基に復号鍵を作成して、再生情報読出部3502から通知された暗号化されたディジタルデータを復号する。なお、その他の構成は、上記実施の形態6のディジタルデータ再生装置の構成とほぼ同様である。

【0119】次に、第2記録媒体3709がこの装置3710に固定的に設けられたICカード等から構成される場合について述べる。この場合には、第2記録媒体3709がこの装置3710以外で再生されることがないことから固有情報取得送出部3707は、媒体識別情報を取得することなく、自ら記憶している機器識別情報を固有情報取得部3705に通知する。また、復号化部3505にも、機器識別情報を通知する。

【0120】このように、第2ディジタルデータ記録再生装置3710に設けられた第2記録媒体3709が着脱自在であるか否かによって、ディジタルデータの暗号化の暗号鍵の作成を媒体識別情報と機器識別情報との組合せによるか、機器識別情報だけで行うかを使い分けることができる。このように使い分けることによっても、ディジタルデータの不正な複製や不正な再生利用を防止することができる。

【0121】次に、本実施の形態の動作を図24に示すフローチャートを用いて説明する。先ず、受信データ1次記録判定部3702は、入力操作部3105からディジタルデータの2次記録の指示が有るのを待ち(S3902)、ディジタルデータの1次記録が許可されているか否かを属性情報3801を見て判断する(S3904)。許可されていないときは、その旨を表示部3104に表示させて(S3906)、処理を終了する。

【0122】許可されているときは、受信データ1次記録判定部3702は、ディジタルデータを1次記録部3703に通知する。1次記録部3703は、第1記録媒体3701にディジタルデータと管理情報を記録する(S3908)。次に、課金情報記録部3109は、1次記録に対して課金されているか否かを判断し(S3910)、1次コピーが有料の時は課金情報を課金情報記録媒体3110に記録する(S3912)。

【0123】次に、受信データ読出判定部3704は、第1記録媒体3701に記録されたディジタルデータの2次記録が許可されているか否かを受信データ1次記録判定部3702に記憶されている属性情報3801を見

て判断する(S3914)。許可されていないときは、2次記録が許可されていない旨を表示部3104に表示させ(S3916)、処理を終了する。

【0124】許可されているときは、受信データ読出判定部3704は、第1記録媒体3701からディジタルデータを読み出し、暗号化部3706に通知するとともに、固有情報取得部3705に第2ディジタルデータ記録再生装置3710から固有情報を取得するよう指示する。固有情報取得部3705は、固有情報を取得し、暗号化部3706に通知する(S3918)。暗号化部3706は、通知された固有情報を基に暗号鍵を作成し(S3920)、通知されているディジタルデータを暗号化して第2ディジタルデータ記録再生装置3710の2次記録部3708に出力する。

【0125】2次記録部3708は、通知された暗号化されたディジタルデータと属性情報と管理情報を第2記録媒体3709に記録する(S3922)。また、課金情報記録部3109は、2次記録に対して課金されているか否かを判断し(S3924)、2次記録が有料のときは、課金情報を課金情報記録媒体3110に記録し(S3926)、処理を終了する。

【0126】なお、第2ディジタルデータ記録再生装置3710でのディジタルデータの再生動作は、実施の形態6のディジタルデータ再生装置の動作とほぼ同様であるので説明を省略する。

(変形例) 上記実施の形態7では、第2記録媒体3709が着脱自在であるときには、第2ディジタルデータ記録再生装置3710の機器識別情報を、第2記録媒体3709の媒体識別情報を組合せた暗号鍵でディジタルデータが暗号化されたけれども、本変形例では、暗号化の形態(媒体識別情報のみに基づいた暗号鍵とするのか媒体識別情報に機器識別情報を組合せた暗号鍵とするのか)をユーザーに指定させ、ユーザーの利用形態の自由度を拡大している。即ち、第2ディジタルデータ記録再生装置3710で第2記録媒体3709に記録された音楽を再生しようとするときには、媒体識別情報及び機器識別情報でディジタルデータを暗号化して記録するようにし、他のディジタルデータ再生装置(媒体識別情報を復号鍵として暗号化されたディジタルデータを復号化できる装置)で第2記録媒体3709に記録された音楽を再生しようとするときには、媒体識別情報でディジタルデータを暗号化して記録するようにする。ユーザーの利用形態に応じて暗号化の形態を選択できるようにしている。

【0127】一方、このユーザーの利用の自由度に応じて2次記録料金を設定して、著作権の保護を図っている。以下、本変形例の具体的構成を説明する。なお、本変形例は、図22に示した第1ディジタルデータ記録装置3700の構成に若干の機能を追加するものであるので、実施の形態7の構成図をそのまま利用して、本変形例固有の構成についてのみ説明する。

【0128】図25は、受信データ1次記録判定部3702に記憶されている属性情報31001の一部を示している。この属性情報31001では、図23に示した属性情報3801の2次記録料金3802と2次記録料金31002との内容が異なる。2次記録料金31002は、暗号化の暗号鍵が媒体識別情報（媒体ID）31003、機器識別情報（機器ID）31004、媒体識別情報と機器識別情報との組合せ31005のいずれであるかによって異なっている。媒体識別情報31003を基に暗号鍵が作成されたものでは、他の装置に第2記録媒体3709を装着して音楽を再生でき、ユーザの自由度が増すことから2次記録料金（2次複製利用料金）が機器識別情報31004又は媒体識別情報と機器識別情報との組合せ31005を基に暗号鍵が作成されたものよりも高額に設定される。ユーザの利用形態の拡大に応じて複製利用料金を課金できるようにしたものである。

【0129】固有情報取得部3705は、固有情報取得送出部3707から機器識別情報と媒体識別情報との通知を受けると、表示部3104に第2記録媒体3709を他の装置で利用するか、第2ディジタルデータ記録再生装置3710でのみ利用するかを表示させ、ユーザの選択を待つ。ユーザは、入力操作部3105より、他の装置を用いるか、第2ディジタルデータ記録再生装置3710のみを用いるかを指定する。即ち、暗号鍵を媒体識別情報だけで作成するか、媒体識別情報と機器識別情報との組合せで作成するかを指示する。

【0130】入力操作部3105は、この指定を固有情報取得部3705と受信データ1次記録判定部3702とに通知する。受信データ1次記録判定部3702は、入力操作部3105から他の装置を用いるとの通知を受けると、課金情報記録部3109に媒体識別情報31003を暗号鍵とする2次記録料金である旨を、第2ディジタルデータ記録再生装置のみを用いるとの通知を受けると、媒体識別情報と機器識別情報との組合せ31005を暗号鍵とする2次記録料金である旨を通知する。

【0131】固有情報取得部3705は、入力操作部3105から、他の装置を用いる旨の通知を受けると、暗号化部3706に媒体識別情報のみを通知する。また、第2ディジタルデータ記録再生装置3710でのみ用いる旨の通知を受けると、同様に媒体識別情報と機器識別情報を通知する。課金情報記録部3109は、暗号化部3706から暗号化されたディジタルデータを2次記録部3708に送出した旨の通知を受けると、受信データ1次記録判定部3702から通知されている属性情報31001の2次記録料金31002を見て、課金情報記録媒体3110に課金情報を記録する。

【0132】なお、本変形例において、第2記録媒体が着脱自在のDVD-RAMであるときには、上記実施の形態6と同様、DVD-RAM固有の識別情報のみを基に暗号鍵を作

成し、ディジタルデータを暗号化して記録するようにできるのは勿論である。また、本変形例の動作は、上記実施の形態7の動作と基本的に異なるところがないのでその説明は省略する。

【0133】なお、上記実施の形態6、7及び変形例において、課金情報記録媒体3110、3508は例えばICカードにより実現し、ディジタルデータの記録や再生時にICカードをセットしなければ動作しないとすることも可能である。また、上記実施の形態6、7及び変形例では、通信部3110で受信されるディジタルデータが音楽データであるとして説明したけれども、これに限ることではなく、映像データ、音声データ、文字データやこれらの組合せであってもよいのは勿論である。

【0134】上記実施の形態6と実施の形態7と変形例のディジタルデータ記録装置及び再生装置並びにディジタルデータ記録再生装置は、図16、図20及び図22にその構成図を示したけれども、各構成要素の機能を発揮するプログラムをコンピュータ読取可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないディジタルデータ記録再生装置に適用して著作権の保護機能を有する装置とすることができる。

#### 【0135】

【発明の効果】以上説明したように、本発明は、ディジタルデータを記録媒体に記録するディジタルデータ記録装置において、暗号化されたディジタルデータをディジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化ディジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでディジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたディジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたディジタルデータを再暗号化させることとしている。

【0136】このような構成によって、再生装置で容易に再生できる暗号化部で再暗号化されたディジタルデータを記録媒体に記録することができ、かつ暗号化されているので著作権の保護を図ることができる。また、前記記録媒体に記録されたディジタルデータは、再生装置により再生され、前記暗号化手段は、前記記録媒体の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第1暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第2暗号化部とを有し、前記制御手段は、前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能などときは、前記第1暗号化部によりディジタルデータの暗号化を行わせ、着脱不可能などときは、前記第2暗号化部によりディジタルデータの暗号化を行わせることとしている。

る。

【0137】このような構成によって、記録媒体がいずれかの再生装置で再生されるときには、その記録媒体の識別情報を基に生成される暗号鍵でディジタルデータを暗号化し、特定の一の再生装置で再生されるときには、その一の再生装置の識別情報を基に生成される暗号鍵でディジタルデータを暗号化することによって、記録媒体に記録されたディジタルデータを再生装置で再生することができる。

【0138】また、前記ディジタルデータ記録装置は、更に、前記ディジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することとしている。このような構成によって、異なるセキュリティレベルを有する暗号化方式の暗号化部を選択することができ、かつ、暗号化部に応じた料金を支払うことができる。

【0139】また、前記制御手段は、前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化ディジタルデータを、前記復号化手段により復号化することを禁止することとしている。このような構成によって、暗号化部で暗号鍵を生成できないときには、ディジタルデータを復号する処理をなくすことができる。

【0140】また、前記暗号化手段の有する複数の暗号化部による暗号化されたディジタルデータは、前記通信手段により受信されたディジタルデータの暗号化に比べいすれもセキュリティレベルが低いこととしている。このような構成によって、再生装置は、ディジタルデータの再生が容易となり、再生装置のコストダウンにつながる。

【0141】また、前記通信手段により受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるディジタルデータは当該ディジタルデータの暗号化方式を示す属性情報を含み、前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたディジタルデータをそれぞれ復号化し、前記制御手段は、前記通信手段により受信された暗号化ディジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化ディジタルデータを復号化するように前記復号化手段を制御することとしている。

【0142】このよな構成によって、受信されたディジタルデータごとに異なるセキュリティレベルを有する暗号化方式で暗号化されていても、暗号化方式に対応した復号化部を選んで、復号化することができる。また、前記ディジタルデータ記録装置は、更に、前記ディジタルネットワークを介して課金処理を行う課金手段を備え、

前記制御手段は、受信した暗号化ディジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することとしている。

【0143】このような構成によって、ディジタルデータの復号化と再暗号化とに対応した利用料金が徴収され、著作権の保護を図ることができる。また、本発明は、ディジタルデータを記録媒体に記録するディジタルデータ記録方法において、暗号化されたディジタルデータをディジタルネットワークを介して受信する通信ステップと、前記通信ステップにより受信された暗号化ディジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたディジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたディジタルデータを前記記録媒体に記録する記録ステップとを有することとしている。

【0144】このような構成によって、再生装置で容易に再生できる暗号化方式で暗号化されたディジタルデータを記録媒体に記録することができ、かつ、暗号化されているので著作権の保護を図ることができる。また、前記通信ステップにより受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるディジタルデータは当該ディジタルデータの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたディジタルデータを復号化することとしている。

【0145】このような構成によって、通信手段で受信された暗号化されたディジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても、復号化することができる。更に本発明は、ディジタルデータを第1記録媒体に記録するディジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、暗号化されたディジタルデータをディジタルネットワークを介して受信する通信ステップと、前記通信ステップにより受信された暗号化ディジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたディジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたディジタルデータを前記第1記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体としている。

【0146】このような構成によって、容易に再生できる暗号化方式で暗号化されたディジタルデータを記録媒体に記録し、かつ、著作権の保護を図る機能のないディジタルデータ記録装置に適用して、このような機能を発

揮させることができる。ここで、前記通信ステップにより受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータは当該データの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたディジタルデータを復号化することをコンピュータに実行させることとしている。

【0147】このような構成によって、通信手段で受信された暗号化されたディジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても復号化することができる。

【図面の簡単な説明】

【図1】本発明に係るディジタルデータ記録装置の実施の形態1の構成図である。

【図2】上記実施の形態のハード構成を示す外観図及び上記実施の形態で得られた記録媒体の再生装置の外観図である。

【図3】上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の一例を示す図である。

【図4】上記実施の形態の一次記録媒体にダウンロードされた音楽データのデータ構造の一例を示す図である。

【図5】上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の他の一例を示す図である。

【図6】上記実施の形態の動作を説明するフローチャートのその1である。

【図7】上記実施の形態の動作を説明するフローチャートのその2である。

【図8】本発明に係るディジタルデータ記録装置の実施の形態2の構成図である。

【図9】上記実施の形態の情報提供者が提供するディジタル信号を記録する際の表示部に表示される情報を示す図である。

【図10】上記実施の形態の動作を示すフローチャートである。

【図11】本発明に係るディジタルデータ記録装置の実施の形態3の構成図である。

【図12】上記実施の形態の情報提供者が提供するディジタル信号の属性情報のデータ構造を示す図である。

【図13】上記実施の形態の動作を示すフローチャートのその1である。

【図14】上記実施の形態の動作を示すフローチャートのその2である。

【図15】本発明に係るディジタルデータ記録装置の実施の形態4の構成図である。

【図16】本発明に係るディジタルデータ記録装置の実施の形態6の構成図である。

【図17】上記実施の形態のディジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

【図18】上記実施の形態の記録媒体に記録される管理情報のデータ構造の一例を示す図である。

【図19】上記実施の形態の動作を説明するフローチャートである。

【図20】上記実施の形態で記録された記録媒体を再生するディジタルデータ再生装置の構成図である。

【図21】上記デジタルデータ再生装置の動作を説明するフローチャートである。

【図22】本発明に係るディジタルデータ記録装置の実施の形態7の構成図である。

【図23】上記実施の形態のディジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

【図24】上記実施の形態の動作を説明するフローチャートである。

【図25】上記実施の形態7の変形例のディジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

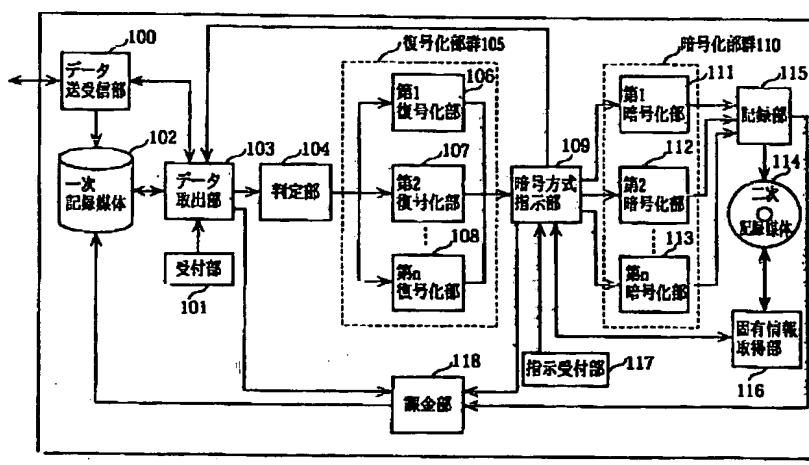
【符号の説明】

100、2101	データ送受信部
101	受付部
102、2102	一次記録媒体
103、2103	データ取出部
104	判定部
105、2115	復号化部群
106	第1復号化部
107	第2復号化部
108	第n復号化部
109	暗号方式指示部
110	暗号化部群
111	第1暗号化部
112	第2暗号化部
113	第n暗号化部
114、2110、3709	二次記録媒体
115、2109、3108	記録部
116、2802、3705	固有情報取得部
117	指示受付部
118、3111	課金部
201	パーソナルコンピュータ
202	DVD-RAMドライブ
203	DVD-RAMディスク
204	DVD-Audioプレーヤ
2104	暗号方式判定部
2105	第1の復号化部
2106	第2の復号化部
2107	第nの復号化部
2108、3706	暗号化部

2111	入力部	3102	記録媒体
2112、3104	表示部	3103	受信データ記録判定部
2113	記録媒体固有情報取得部	3105	入力操作部
2401	属性情報取得部	3119	課金情報記録部
2402	コピー制御情報検出判定部	3110	課金情報記録媒体
2403	コピー制御情報変換部	3700	第1デジタルデータ記録装置
2404	課金情報算出部	3701	第1記録媒体
2800	第1のデジタルデータ記録装置	3703	1次記録部
2801	第2のデジタルデータ記録装置	3704	受信データ読出判定部
2803、3707	固有情報取得送出部	3710	第2デジタルデータ記録再生装置
3101	通信部		

【図1】

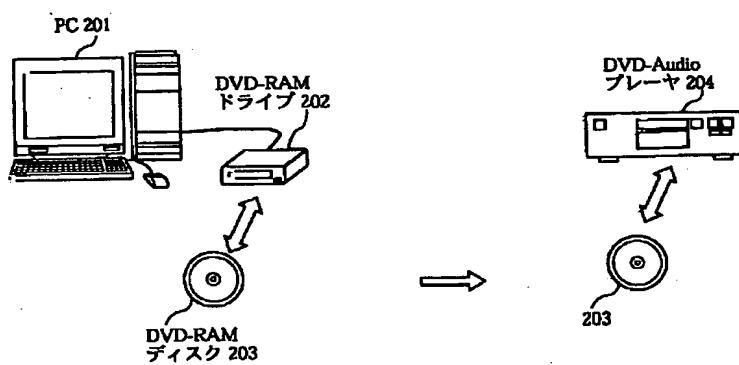
【図18】



管理情報 3301		
曲名コード	記録開始アドレス	記録終了アドレス
song01	00320	00933
song02	14902	15172
song03	13085	13994
song04	50870	51825
song05	58349	58783

デジタルデータ記録装置

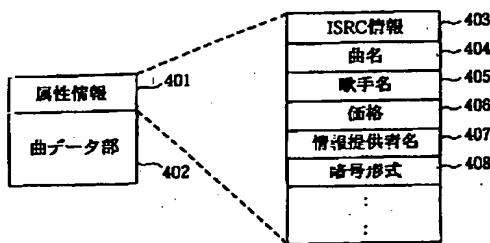
【図2】



【図3】

301	302	303	304
曲名	歌手名	収録時間	価格
Song1	SingerA	4分20秒	100円
Song2	SingerB	3分53秒	50円
Song3	SingerC	4分48秒	75円
Song4	SingerD	4分06秒	100円
:	:	:	:
:	:	:	:

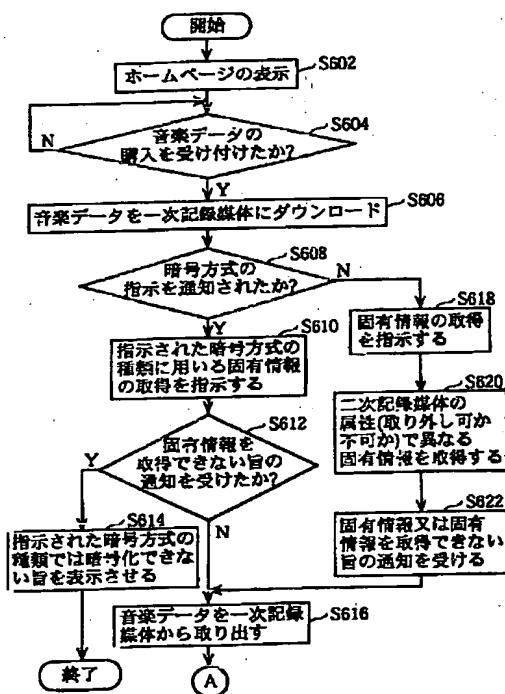
【図4】



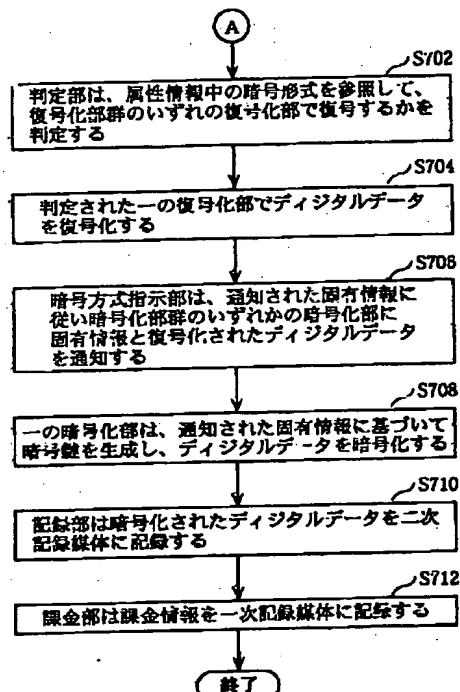
【図5】

曲名	歌手名	収録時間	価格(1)	価格(2)
301	302	303	501	502
Song1	SingerA	4分20秒	100円	70円
Song2	SingerB	3分53秒	50円	35円
Song3	SlugerC	4分48秒	75円	50円
Song4	SlugerD	4分06秒	100円	100円
:	:	:	:	:
:	:	:	:	:

【図6】



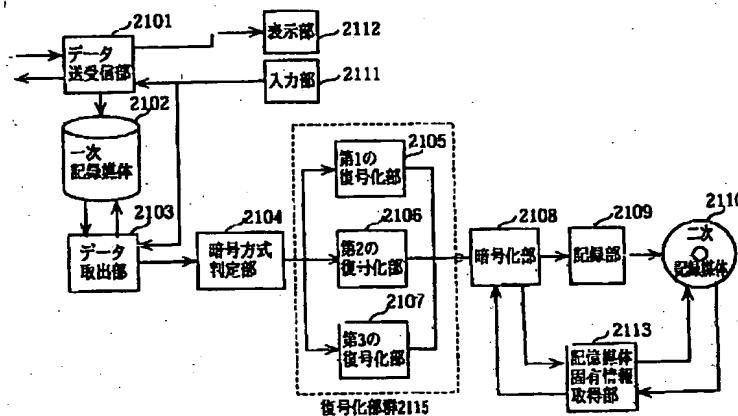
【図7】



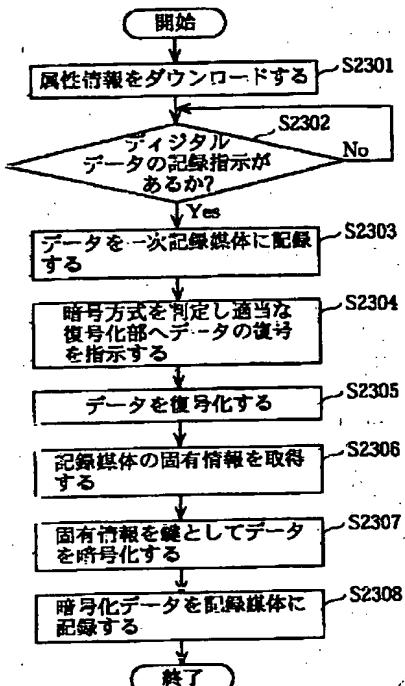
【図9】

曲名	曲名コード	歌手名	データ入手先
2201	2202	2203	2204
曲A	song01	A	www.song/song01
曲B	song02	B	www.song/song02
曲C	song03	C	www.song/song03
曲D	song04	D	www.song/song04
曲E	song05	E	www.song/song05

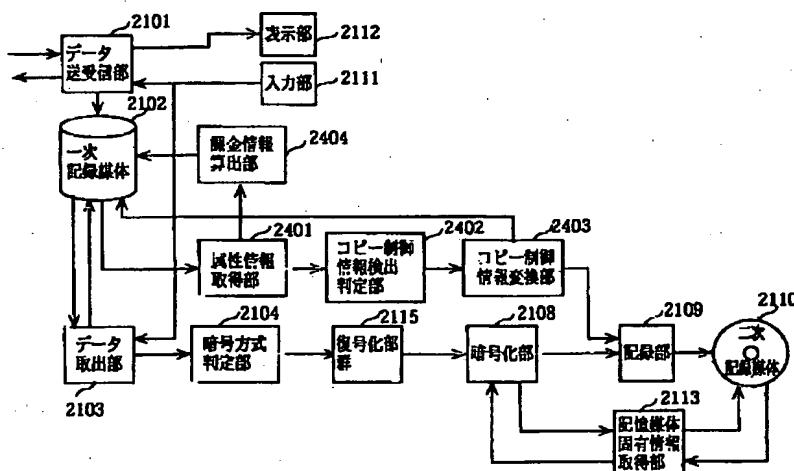
【図8】



【図10】



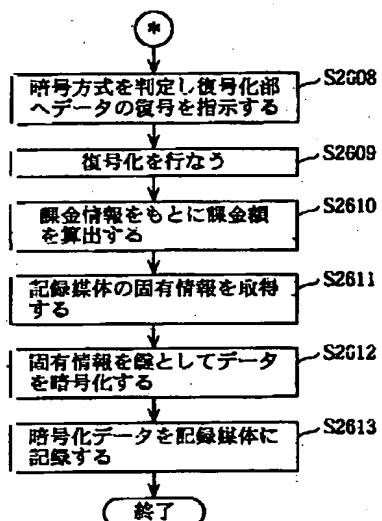
【図11】



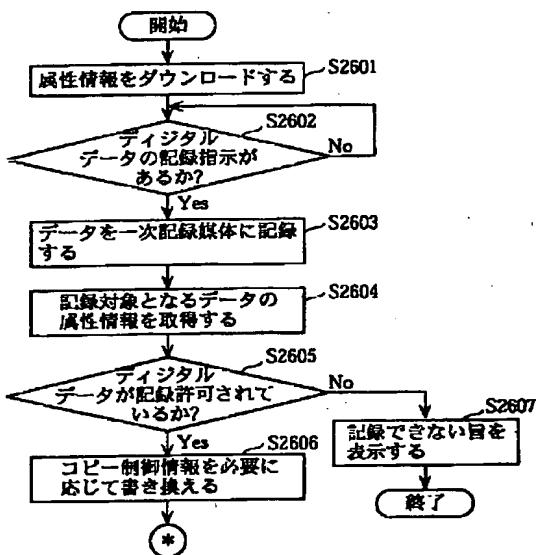
【図12】

曲名	曲名コード	歌手名	データ入手先	コピー制御情報	価格
曲A	song01	A	www.song/song01	孫コピー不可	100円
曲B	song02	B	www.song/song02	無制限に許可	10円
曲C	song03	C	www.song/song03	孫コピー不可	0円
曲D	song04	D	www.song/song04	孫コピー不可	30円
曲E	song05	E	www.song/song05	2回コピー可	10円

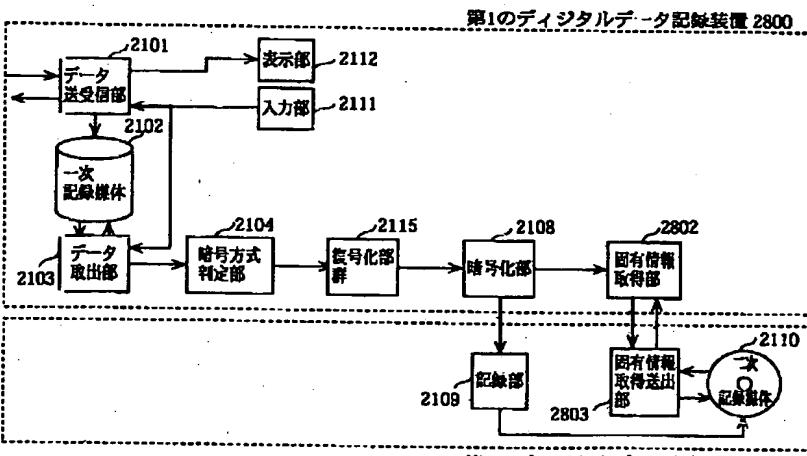
【図14】



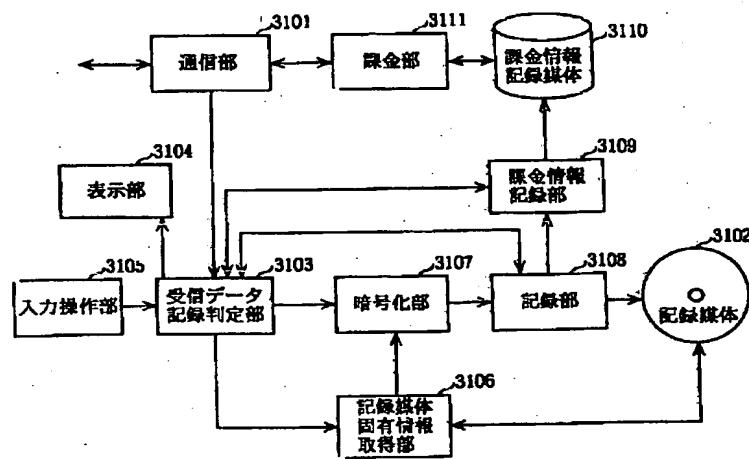
【図13】



【図15】



【図16】



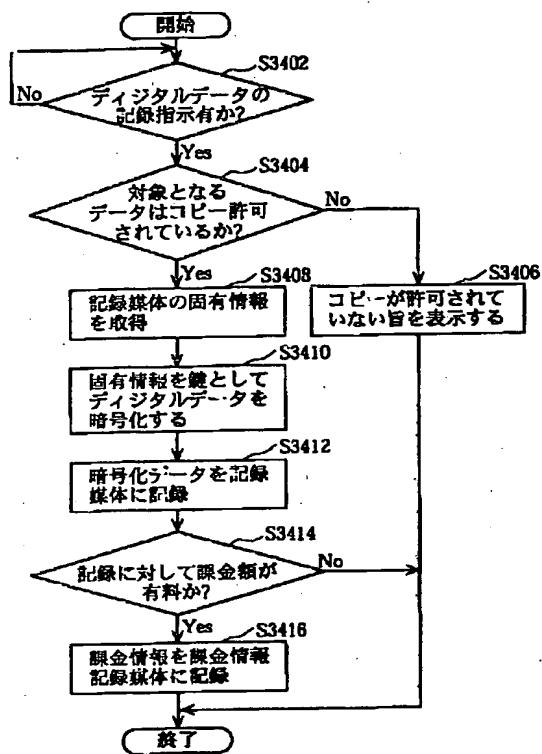
【図17】

属性情報 3201									
曲名	演奏者	曲名コード	記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可	...	3202 3203 3204 3205 3206 3207 3208 3209
曲A	a	song01	100円	0.5円	100回	暗号あり	1回のみ可	...	
曲B	b	song02	10円	0円	無限	暗号なし	許可	...	
曲C	c	song03	0円	1円	50回	暗号あり	1回のみ可	...	
曲D	d	song04	30円	5円	50回	暗号あり	1回のみ可	...	
曲E	e	song05	10円	0円	10回	暗号なし	許可	...	

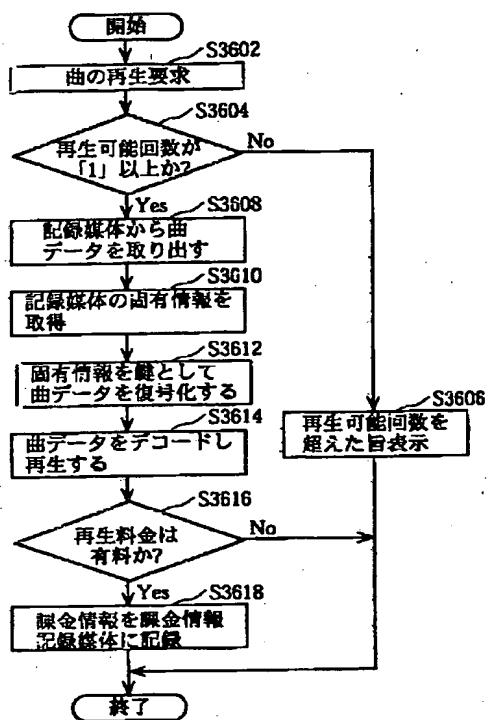
【図23】

属性情報 3801										3805 3802 3803 3804
曲名	演奏者	曲名コード	1次記録料金	2次記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可(1次)	コピー許可(2次)	3805 3802 3803 3804
曲A	a	song01	0円	100円	0.5円	100回	暗号あり	1回のみ可	1回のみ可	
曲B	b	song02	10円	10円	0円	無限	暗号なし	許可	許可	
曲C	c	song03	0円	0円	1円	50回	暗号あり	1回のみ可	1回のみ可	
曲D	d	song04	0円	30円	5円	50回	暗号あり	1回のみ可	1回のみ可	
曲E	e	song05	—	—	—	—	暗号なし	不許可	不許可	

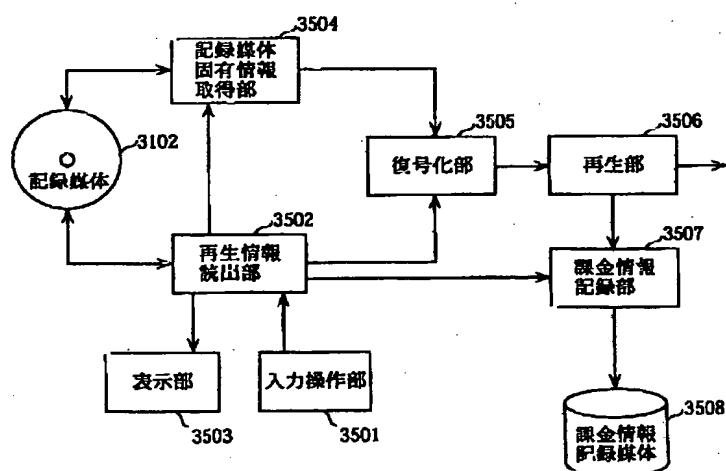
【図19】



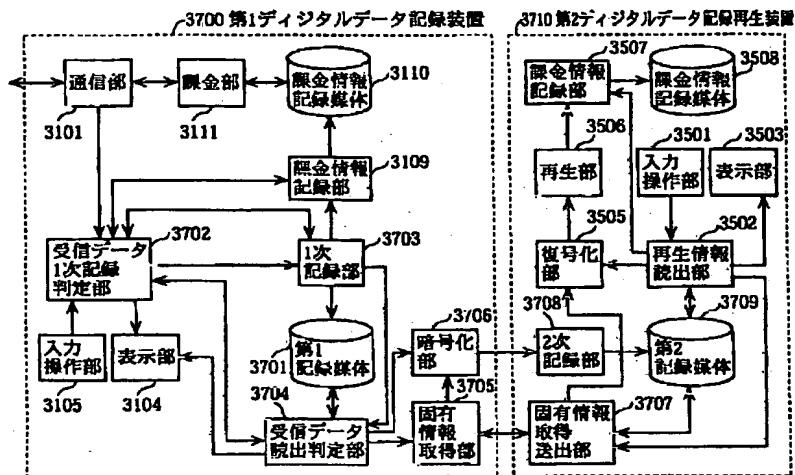
【図21】



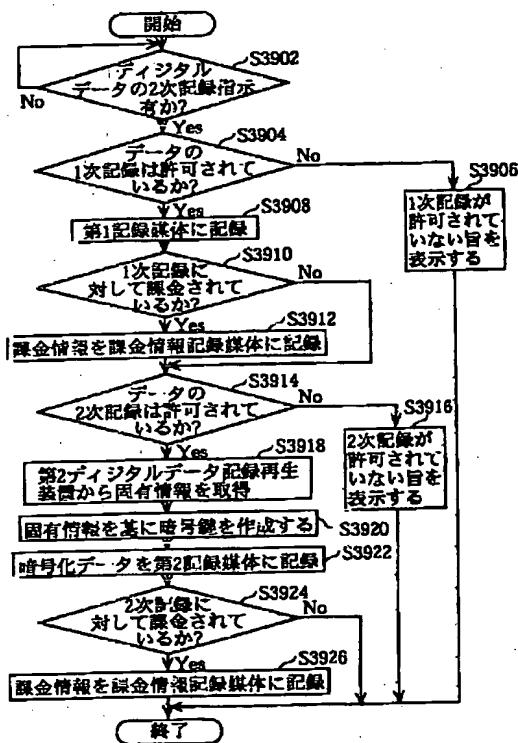
【図20】



【図22】



【図24】



(27) 00-187935 (P2000-187935A)

【図25】

...	曲名 コード	...	2次記録料金			...
			媒体ID	機器ID	媒体ID+機器ID	
...	song01	...	100円	10円	10円	...
...	song02	...	10円	1円	1円	...
...	song03	...	0円	0円	0円	...
...	song04	...	30円	3円	3円	...
...	song05	...	10円	1円	1円	...

属性情報31001

31003 31002 31004

31005

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**